HOTWIRE™ 7986 M/HDSL STANDALONE TERMINATION UNIT

WITH G.703 INTERFACE

USER'S GUIDE

Document No. 7986-A2-GB20-10

December 1998

PARADYNE™

Copyright © 1998 Paradyne Corporation.
All rights reserved.
Printed in U.S.A.

Notice

This publication is protected by federal copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission of Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773.

Paradyne Corporation makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, Paradyne Corporation reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Paradyne Corporation to notify any person of such revision or changes.

Changes and enhancements to the product and to the information herein will be documented and issued as a new release to this manual.

Warranty, Sales, and Service Information

Contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- **Via the Internet:** Visit the Paradyne World Wide Web site at http://www.paradyne.com
- **Via Telephone:** Call our automated call system to receive current information via fax or to speak with a company representative.
  - — Within the U.S.A., call 1-800-870-2221
  - — Outside the U.S.A., call 1-727-530-2340

Trademarks

All products and services mentioned herein are the trademarks, service marks, registered trademarks or registered service marks of their respective owners.

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773, or send e-mail to userdoc@eng.paradyne.com. Include the number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

Printed on recycled paper

Important Safety Instructions

1. Read and follow all warning notices and instructions marked on the product or included in the manual.
2. Input power to this product must be provided by one of the following: (1) a UL Listed/CSA Certified power source with a Class 2 or Limited Power Source (LPS) output for use in North America; or (2) a 24 Vdc National Electric Code (NEC) ANSI/NFPA 70/Canadian Electric Code (CEC) Class 2 circuit installed in accordance with articles 110-16, 110-17, and 110-18 of the NEC, and articles 2-308, 2-310, 2-312, 2-314, 2-200, and 2-202 of the CEC, or (3) a Safety Extra Low Voltage (SELV) power source with a maximum available output of less than 240 VA, certified for use in the country of installation.
3. Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the product and to protect it from overheating, these slots and openings must not be blocked or covered.
4. Do not allow anything to rest on the power cord and do not locate the product where persons will walk on the power cord.
5. Do not attempt to install or service this product yourself, as opening or removing covers may expose you to dangerous high voltage points or other risks. Refer all installation and servicing to qualified service personnel.
6. General purpose cables are provided with this product. Special cables, which may be required by the regulatory inspection authority for the installation site, are the responsibility of the customer.
7. When installed in the final configuration, the product must comply with the applicable Safety Standards and regulatory requirements of the country in which it is installed. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.
8. A rare phenomenon can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate buildings are **interconnected**, the voltage potential may cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action prior to interconnecting the products.
9. In addition, if the equipment is to be used with telecommunications circuits, take the following precautions:
   - Never install telephone wiring during a lightning storm.
   - Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
   - Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
   - Use caution when installing or modifying telephone lines.
   - Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
   - Do not use the telephone to report a gas leak in the vicinity of the leak.

EMI Warnings

⚠ WARNING:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The authority to operate this equipment is conditioned by the requirements that no modifications will be made to the equipment unless the changes or modifications are expressly approved by Paradyne Corporation.

⚠ WARNING:

To Users of Digital Apparatus in Canada:

This Class A digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du règlement sur le matérial brouilleur du Canada.

Contents

About This Guide

- Document Purpose and Intended Audience v
- Document Summary v
- Product-Related Documents vi

1 About the Hotwire 7986 Standalone Termination Unit

- M/HDSL Overview 1-1
- Hotwire 7986 Termination Unit Features 1-2
- Network Configuration 1-3
- Front Panel LED Status Indicators 1-4
- Rear Panel Interface Connections 1-4
- SNMP Management Capabilities 1-5
  - Management Information Base (MIB) Support 1-5
  - SNMP Trap Support 1-5

2 Using the Asynchronous Terminal Interface

- User Interface Access 2-1
- Communication Port Settings 2-1
- Initiating an ATI Session 2-2
- Screen Work Areas 2-5
- Navigating the Screens 2-6
  - Keyboard Keys 2-6
  - Screen Function Keys 2-7
  - Switching Between Screen Work Areas 2-8
- Ending an ATI Session 2-9

3 Initial Startup and Configuration

- Overview 3-1
- Connecting Power to the Unit 3-2
- Optional Power Sources 3-2
  - Connecting the Unit to an Optional External DC Power Source 3-2
- Connecting to the Network 3-3
- Connecting to a System Terminal 3-3
- Entering Identity Information 3-4
- Choosing a Configuration Mode 3-6
- Configuring the Unit Using the Configuration Menus 3-6
  - Configuration Options 3-6
- Configuring the Unit Using the Internal Switches 3-7
  - Switchpack Locations 3-8
  - Switchpack Definitions 3-9
- Accessing and Displaying Configuration Options 3-11
- Configuration Edit/Display 3-12
- Configuring AutoRate 3-13
- Configuration Loader 3-15
- Saving Configuration Options 3-17
- Download Code 3-18

4 Monitoring the Unit

- What to Monitor 4-1
- Viewing System and Test Status 4-2
  - Health and Status 4-3
  - Self-Test Results 4-5
  - Test Status 4-6
- Viewing Network Error Statistics 4-7
- Viewing Network Performance Statistics 4-9
- Viewing G.703 Performance Statistics 4-11
- Viewing 7986 Standalone Termination Unit LEDs 4-13
- Hotwire 7986 Standalone Termination Unit LEDs 4-14

5 Testing

- Accessing the Test Menu 5-1
- Running Network Tests 5-2
  - Line Loopback 5-3
  - Repeater Loopback 5-4
  - DTE Loopback 5-5
  - Send Remote Line Loopback 5-6
  - Send and Monitor 511 5-7
- Device Tests 5-8
  - Lamp Test 5-8
- Ending an Active Test 5-9

6 Messages and Troubleshooting

- Overview 6-1
- Configuring SNMP Traps 6-2
- Device Messages 6-3
- Troubleshooting 6-5

7 Security

- Overview 7-1
- ATI Access Levels 7-1
- Creating a Login 7-2
- Deleting a Login 7-4
- Controlling SNMP Access 7-4
  - Assigning SNMP Community Names and Access Types 7-4
  - Limiting SNMP Access through the IP Addresses of the Managers . 7-5
- Resetting the Termination Unit's COM Port or Factory Defaults 7-5

8 IP Addressing

- Selecting an IP Addressing Scheme 8-1
- IP Addressing Example 8-2

A Configuration Option Tables

- Overview A-1
- Network Interface Options Menu A-2
- G.703 Interface Options Menu A-4
- System Options Menu A-6
- Communication Port A-8
- Management and Communication Options Menu A-11
  - Telnet Session Options A-11
  - Communication Protocol Options A-13
  - SNMP Traps Options A-16
  - General SNMP Management Options A-19
  - SNMP NMS Security Options A-21

B Standards Compliance for SNMP Traps

- SNMP Traps B-1
  - warmStart B-1
  - authenticationFailure B-1
  - linkUp and linkDown B-2
- Enterprise-Specific Traps B-3

C Cables and Pin Assignments

- Overview C-1
- E1 Network Interface C-2
- DSL Network Interface Cable C-3
- COM Port Interface Cable C-4
- Power Input Connector C-5
- Optional Power Cable C-5

D Technical Specifications

Glossary

Index

About This Guide

Document Purpose and Intended Audience

This guide contains information needed to set up, configure, and operate the Hotwire 7986 Multirate High-bit-rate Digital Subscriber Line (M/HDSL) Standalone Termination Unit with G.703 interface and is intended for installers and operators.

Document Summary

Section	Description
Chapter 1	*About the 7986 Standalone Termination Unit.* Describes the 7986 Termination Unit's features and capabilities.
Chapter 2	*Using the Asynchronous Terminal Interface.* Provides instructions for accessing the user interface and navigating through the screens.
Chapter 3	*Initial Startup and Configuration.* Provides procedures for setting up the user interface and configuration steps.
Chapter 4	*Monitoring the Unit.* Describes using the LEDs, status, and network statistics to monitor the unit.
Chapter 5	*Testing.* Provides information about available tests and test setup.
Chapter 6	*Messages and Troubleshooting.* Provides information on SNMP traps, device messages, and troubleshooting.
Chapter 7	*Security.* Presents procedures for creating a login, setting the effective access levels, and controlling SNMP access.
Chapter 8	*IP Addressing.* Provides information and examples regarding IP addresses.

Section	Description
Appendix A	*Configuration Option Tables.* Contains all configuration options, default settings, and possible settings.
Appendix B	*Standards Compliance for SNMP Traps.* Contains SNMP trap compliance information.
Appendix C	*Cables and Pin Assignments.* Contains connector and interface information.
Appendix D	*Technical Specifications.* Contains physical and regulatory specifications, network and port interfaces, power consumption values, and accessory part numbers.
Glossary	Defines acronyms and terms used in this document.
Index	Lists key terms, acronyms, concepts, and sections in alphabetical order.

Product-Related Documents

Document Number	Document Title
8786-A2-GB20	*Hotwire 8786 M/HDSL Termination Unit User's Guide*
8786-A2-GZ40	*Hotwire 8786 M/HDSL Termination Unit Installation Instructions*

Contact your sales or service representative to order additional product documentation.

Paradyne documents are also available on the World Wide Web at:

http://www.paradyne.com

Select *Service & Support* → *Technical Manuals*

About the Hotwire 7986 Standalone Termination Unit

1

M/HDSL Overview

Hotwire™ Multirate High-bit-rate Digital Subscriber Line (M/HDSL) products maximize customer service areas by varying the DSL line rate. This ensures symmetric DSL connectivity over a wide range of telephone line distances and transmission line qualities.

Hotwire M/HDSL products can transport at full or fractional payload rates over a 4-wire, full-duplex circuit over varying distances based on the conditions of the 4-wire loop. Examples include support for router, multiplexer and PBX connections at 128 kbps, with distances exceeding 21,000 feet (6.9 km) on 24 gauge (.5 mm) cable delivered at 2.048 Mbps.

Hotwire M/HDSL units are equipped with an automatic configuration capability that reduces the M/HDSL installation process to a simple plug and play mode. Simply connecting the units to the line automatically configures the customer for the maximum data rate supported by the local loop. M/HDSL units can also be configured at fixed line speeds.

Hotwire 7986 Termination Unit Features

The Hotwire 7986 M/HDSL Standalone Termination Unit is an endpoint for the chassis-mounted Hotwire 8786 M/HDSL Termination Unit housed in the Hotwire 8600 or 8800 Digital Subscriber Line Access Multiplexer (DSLAM).

Two Hotwire 7986 M/HDSL Standalone Termination Units can also be configured to operate in a central office LTU to customer premises NTU environment.

The 7986 Standalone Termination Unit offers these standard features:

- **AutoRate Capability.** Provides automatic configuration of line speed and data rate upon connection.
- **Embedded Operations Channel (EOC).** Provides remote SNMP Traps or Telnet session capability over the M/HDSL link.
- **Asynchronous Terminal Interface (ATI).** Provides a menu-driven VT100-compatible terminal interface for configuring and managing the termination unit locally or remotely by Telnet session.
- **Local Management.** Provides local management using a:
  - — Terminal or equivalent through the COM port of the unit
  - — NMS connection through the 10BaseT port
- **Remote Management.** Provides remote management using:
  - — VT100 Terminal or PC via the Management Serial port of the DSLAM
  - — Network Management System (NMS) via the COM port or MCC port of the DSLAM
  - — Telnet over the EOC
  - — External modem out-of-band
  - — Using SNMP or Telnet through the 10BaseT port or the Internal Management Channel (IMC)
- **Alarm Indication.** Provides front panel status LEDs.
- **Diagnostic Testing.** Provides the capability to diagnose device and network problems and perform digital loopbacks, pattern tests, and self-test.
- **Device and Performance Monitoring.** Provides the capability of tracking and evaluating the unit's operation, including health and status, and error-rate monitoring.

Network Configuration

Figure 1-1 shows a network application using a 2-port Hotwire 8786 M/HDSL Termination Unit for access concentration in a central office (CO). A frame relay switch and a router are connected, through the termination unit, to partner units supporting a host or router, and frame relay encapsulated or unframed data.

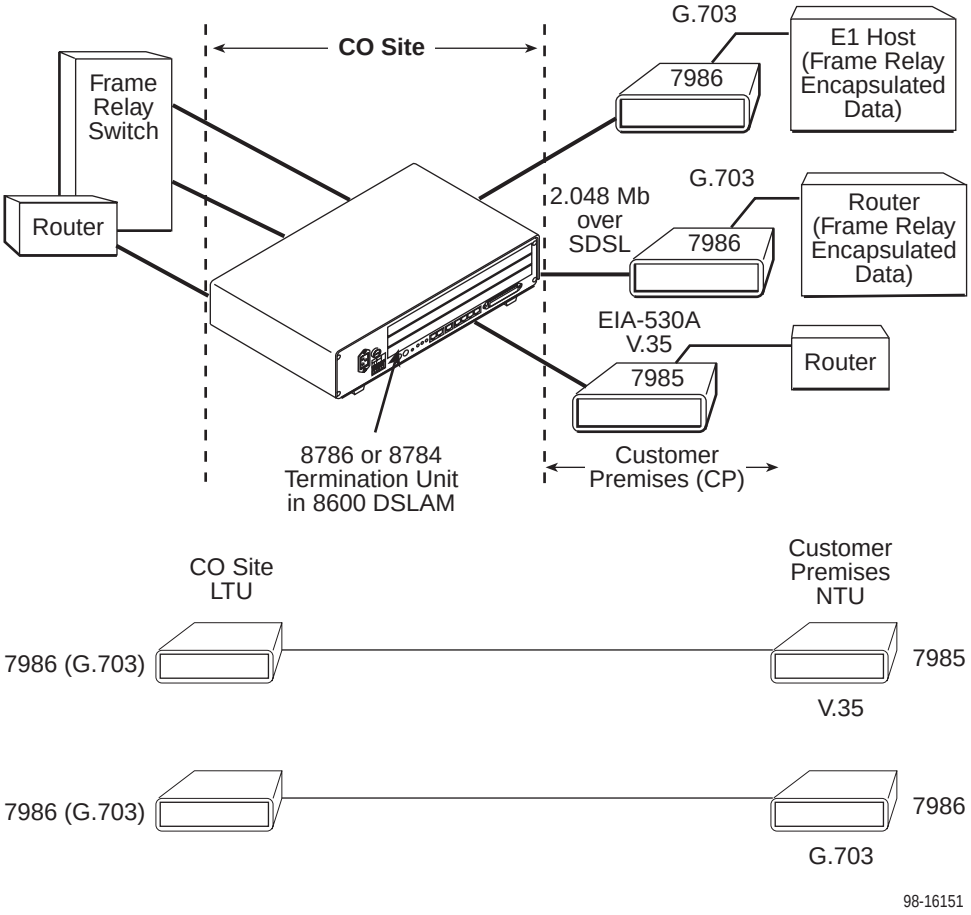


Figure 1-1. Sample M/HDSL Configurations

NOTE:

A crossover cable (Pins 1, 2 to 4, 5) is required for connecting two 7986 Termination Units back-to-back.

Front Panel LED Status Indicators

Figure 1-2 shows the front panel of the 7986 Standalone Termination Unit. For more information on front panel LEDs, refer to Chapter 4, *Monitoring the Unit*.

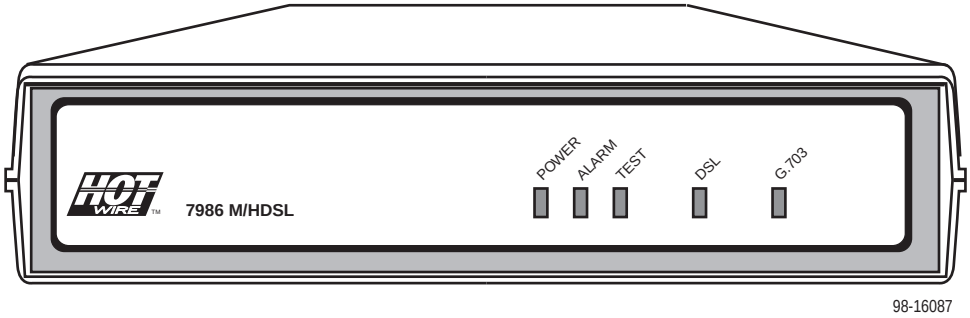


Figure 1-2. Hotwire 7986 Standalone Termination Unit Front Panel

Rear Panel Interface Connections

Figure 1-3 shows the physical interfaces of the 7986 Standalone Termination Unit.

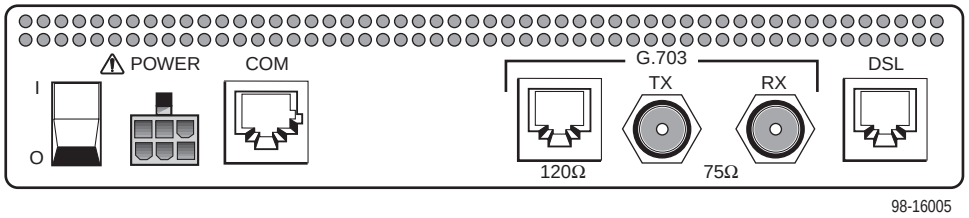


Figure 1-3. Hotwire 7986 Standalone Termination Unit Rear Panel

SNMP Management Capabilities

The termination unit supports SNMP Version 1, and can be managed by any industry-standard SNMP manager and accessed using SNMP by external SNMP managers.

Management Information Base (MIB) Support

For a detailed description of supported MIBs, visit Paradyne's web site at **http://www.paradyne.com**. The following MIBs are supported:

- **MIB II (RFC 1213 and RFC 1573)** – Defines the general objects for use with a network management protocol in TCP/IP internets and provides general information about the unit. MIB II is backward-compatible with MIB I.
- **DS1/E1 MIB (RFC 1406)** – Reports the performance status of the DSX-1 interface and supports the features found on the DSX-1 Performance Statistics screen.
- **RS-232-Like MIB (RFC 1659)** – Defines objects for managing RS-232-type interfaces (e.g., V.35, RS-422, RS-423, etc.) and supports the synchronous data port on the DSU.
- **Enterprise MIB** – Supports configuration, status, statistics, and tests.

SNMP Trap Support

The 7986 Standalone Termination Unit supports traps as defined in RFC 1215. They may include variable-bindings specified in the following MIBs:

- **MIB II (RFC 1573)** – Defines the general objects for use with a network management protocol in TCP/IP internets and provides general information about the 7986 Standalone Termination Unit.
- **Enterprise MIB** – Supports configuration, status, statistics, and tests.

Figure 1-4 illustrates a typical M/HDSL SNMP configuration. Refer to Chapter 8, *IP Addressing* and Appendix B, *Standards Compliance for SNMP Traps*.

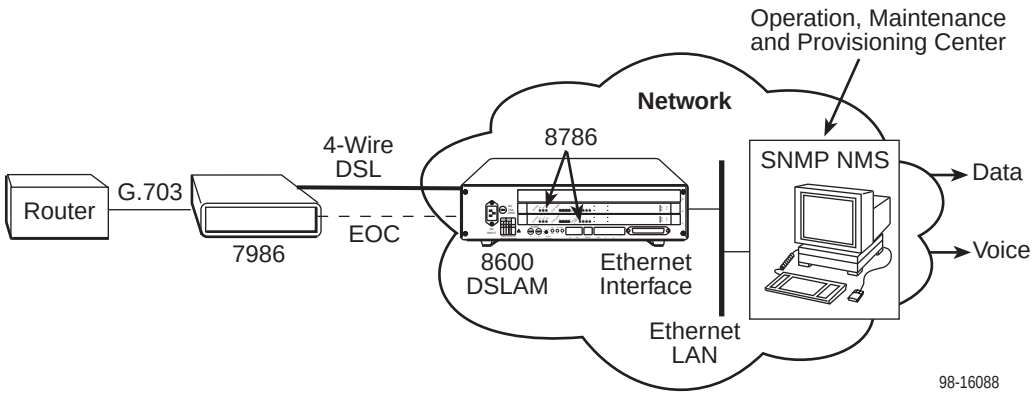


Figure 1-4. M/HDSL SNMP Configuration

Figure 1-5 illustrates an M/HDSL SNMP configuration connected directly to the Communications Port. Refer to Chapter 8, *IP Addressing* and Appendix B, *Standards Compliance for SNMP Traps*.

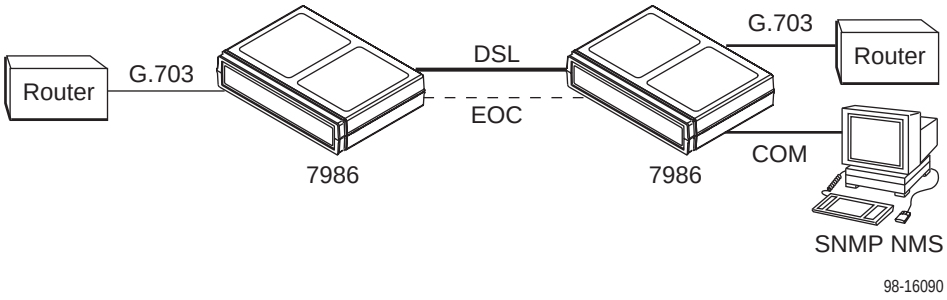


Figure 1-5. M/HDSL Local SNMP Configuration

Using the Asynchronous Terminal Interface

2

User Interface Access

You can communicate with the Hotwire 7986 Standalone Termination Unit with an asynchronous terminal interface (ATI) using one of the following methods:

- Direct connection through the COM port.
- Telnet session through the Embedded Operations Channel (EOC).

NOTE:

Only one terminal interface session can be active at a time, and another user's session cannot be forced to end. To automatically log out a user due to inactivity, enable the Inactivity Timeout option (see Table A-5, Telnet Session Options, in Appendix A, *Configuration Option Tables*).

Security can limit ATI access several ways. To limit user access or set up login IDs, refer to Chapter 7, *Security*.

Communication Port Settings

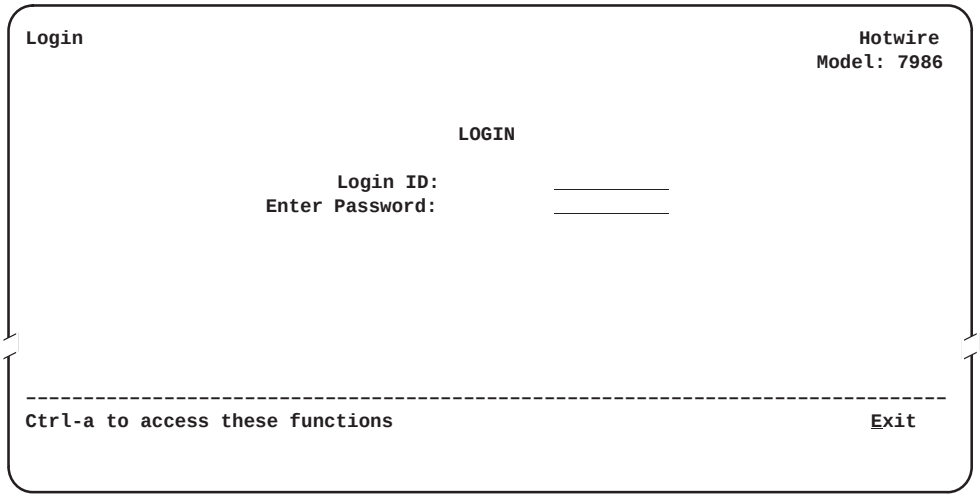
Ensure that the device you connect communicates using these settings:

- Data rate set to 9.6 kbps.
- Character length set to 8.
- Parity set to None.
- Stop Bits set to 1.

Initiating an ATI Session

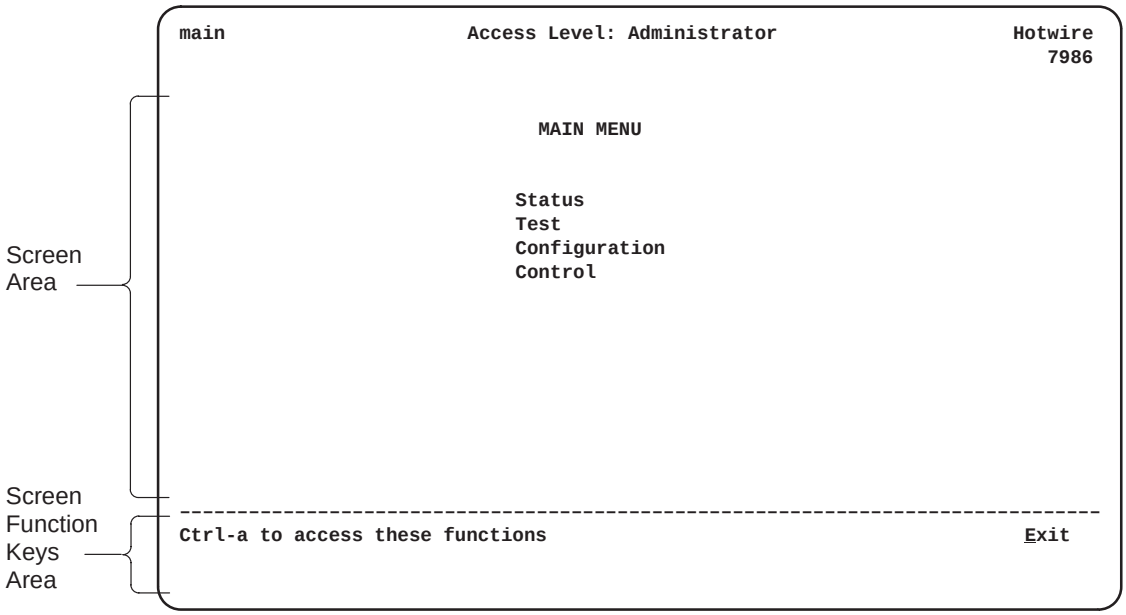
The Main Menu screen is displayed on the screen unless a login ID and password is required or the ATI is already in use.

If security is enabled on the 7986 Standalone Termination Unit and you used Telnet to access it directly (you did not log in through the MCC), the system prompts you for a login ID and password.



After you enter a valid login ID and password, the Main Menu appears. If you enter an invalid login ID and password after three attempts, the Telnet session closes or the terminal connection returns to an idle state. Refer to Chapter 7, *Security*.

If the ATI is already in use, you will see a **`connection refused`** or **`connection failed`** message (if you are using a Telnet session), or you will see the IP address of the other user (if you are using the Management Serial port).



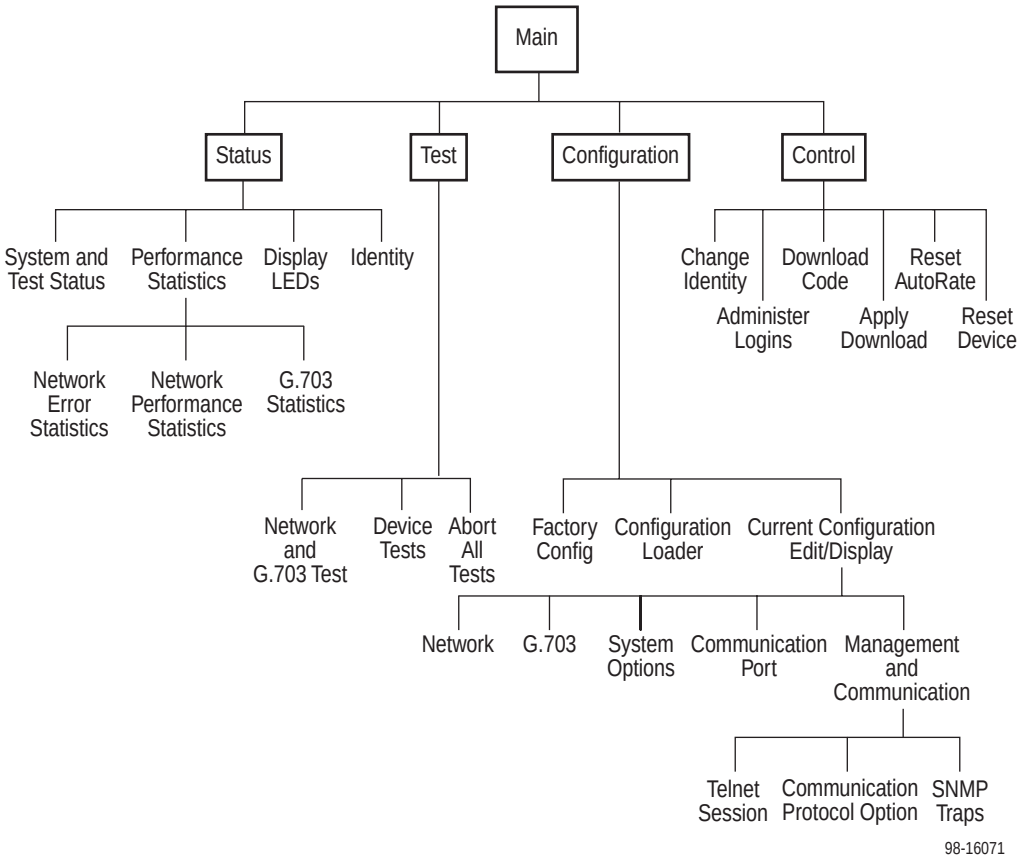
Entry to all of the termination unit's tasks begins at the Main Menu screen. The four branches of the Main menu are as follows:

Select . . .	To . . .
Status	View system status, diagnostic test results, statistics, LEDs, and device identity information.
Test	Select and cancel tests for the termination unit's interfaces.
Configuration	Display and edit the configuration options.
Control	Change the device identity, administer logins, download new firmware, or initiate a power-up reset of the termination unit.

After selecting an option, what appears on the screens depends on the:

- **Current configuration** – How your termination unit is currently configured.
- **Effective security access level** – An access level that is typically set by the system administrator for each interface and each user.
- **Data selection criteria** – What you entered in previous screens.

The following illustration shows the menu paths to the different ATI screens.



Screen Work Areas

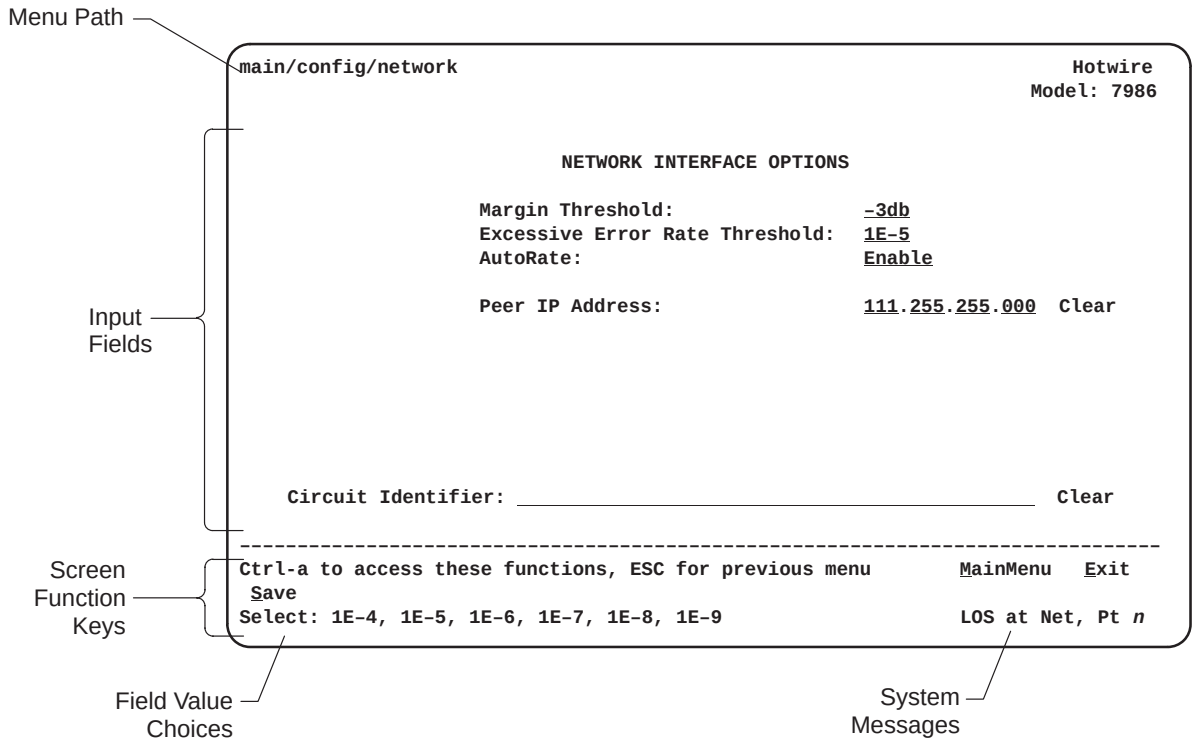
There are two user work areas:

- **Screen area** – This is the area above the dotted line that provides the menu path, menus, and input fields.

  The menu path appears as the first line on the screen. In this manual, the menu path is presented as a menu selection sequence with the names of the screens:

  Main Menu → Configuration → Load Configuration From → Network Interface Options

- **Screen function key area** – This is the area below the dotted line that lists function keys specific to the screen, field value choices, and system messages.



Navigating the Screens

You can navigate the screens by:

- Using keyboard keys
- Using screen function keys
- Switching between the two screen work areas

Keyboard Keys

Use the following keyboard keys to navigate within the screen.

Press . . .	To . . .
Ctrl-a	Move cursor between the screen area and the screen function keys area below the dotted line at the bottom of the screen.
Esc	Return to the previous screen.
Tab	Move cursor to the next field on the screen.
Backspace	Move cursor to the previous field on the screen.
Return (Enter)	Accept entry or display valid options on the last row of the screen when pressed before entering data or after entering invalid data.
Ctrl-k	Tab backwards (move cursor one field to the left).
Spacebar	Select the next valid value for the field.
Delete (Del)	Delete character that the cursor is on.
Up Arrow or Ctrl-u	Move cursor up one field within a column on the same screen.
Down Arrow or Ctrl-d	Move cursor down one field within a column on the same screen.
Right Arrow or Ctrl-f	Move cursor one character to the right if in edit mode.
Left Arrow or Ctrl-b	Move cursor one character to the left if in edit mode.
Ctrl-l	Redraw the screen display, clearing information typed in but not yet entered.

▶ Procedure

To make a menu or field selection:

1. Press the Tab key or the right arrow key to position the cursor on a menu or field selection. Each selection is highlighted as you press the key to move the cursor from position to position.
2. Press Enter.

   The selected menu or screen appears.
3. Continue Steps 1 and 2 until you reach the screen you want.

The current setting or value appears to the right of the field name. You can enter information into a selected field by:

- Typing in the first letter(s) of a field value or command.
- Switching from the screen area to the screen function area below the dotted line and selecting or entering the designated screen function key.

If a field is blank and the Field Values screen area displays valid selections, press the spacebar and the first valid value for the field will appear. Continue pressing the spacebar to scroll through other valid values.

Screen Function Keys

All screen function keys located below the dotted line operate the same way (upper- or lowercase) throughout the screens.

For the screen function . . .	Select . . .	And press Enter to . . .
ClrFar	F or f	Clear far-end network statistics and refresh the screen.
ClrNear	N or n	Clear near-end network statistics and refresh the screen.
Delete	L or l	Delete data.
Exit	E or e	Terminate the async terminal session.
MainMenu	M or m	Return to the Main Menu screen.
New	N or n	Enter new data.
PgDn	D or d	Display the next page, or group of entries.
PgUp	U or u	Display the previous page, or group of entries.
ResetMon	R or r	Reset an active Monitor 511 test counter to zero.
Save	S or s	Save information.

Switching Between Screen Work Areas

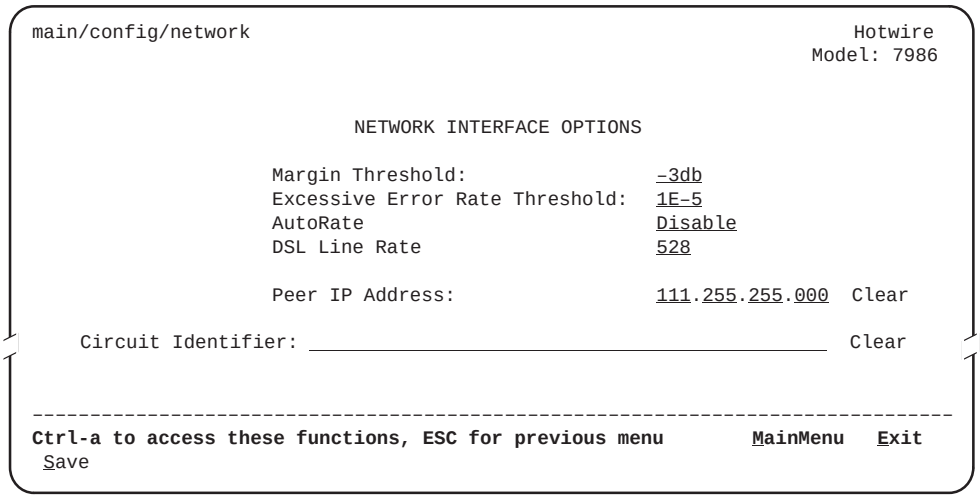
Select Ctrl-a to switch between the two screen work areas to perform all screen functions.

▶ Procedure

To access the screen function area below the dotted line:

1. Press Ctrl-a to switch from the screen area to the screen function key area below the dotted line.
2. Select either the function's designated (underlined) character or press the Tab key until you reach the desired function key.

   Example:
   To save the current screen, type **s** or **S** (Save).
3. Press Enter.
4. To return to the screen area above the dotted line, press Ctrl-a again.



Ending an ATI Session

Use the Exit function key from any screen to terminate the session.

▶ Procedure

To end a session with the asynchronous terminal interface:

1. Press Ctrl-a to go to the screen function key area below the dotted line.
2. Save changes if required. A confirmation message appears if you have made but not saved changes to your configuration.
3. Tab to Exit (or type **e** or **E**) and press Enter.

Initial Startup and Configuration

3

Overview

This chapter provides instructions on how to access and configure your unit for the first time. This chapter includes procedures for:

- Connecting power to the unit.
- Connecting the unit to the network.
- Connecting a system terminal.
- Providing initial unit identity information or changing existing identity information.
- Configuring your unit using internal switchpacks or using the Configuration Edit menus.
- Choosing the current or factory default configuration options or downloading configuration options from a TFTP server.
- Modifying current configuration options using the Configuration Edit/Display menu.
- Saving your changes.
- Downloading unit firmware from a TFTP server.

Connecting Power to the Unit

If your package includes a power pack: Plug the power pack into an ac outlet having a nominal voltage rating between 100–240 Vac. Connect the output cable of the power pack to the connector marked POWER on the rear panel.

If your package includes a direct-connection dc power cable: Connect the unit to an external dc power source as described in *Connecting the Unit to an Optional External DC Power Source*.

Optional Power Sources

Using the optional dc power cable, the unit is capable of operating on a +24 Vdc power source. To select the power, choose one of the following power supply types.

Connecting the Unit to an Optional External DC Power Source

Using the dc power cable, the Hotwire 7986 Standalone Termination Unit is capable of operating on a +24 Vdc power supply.

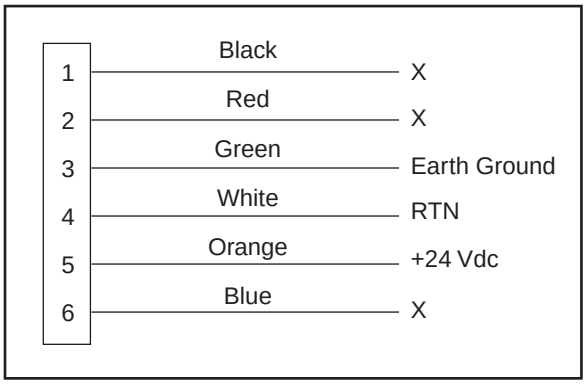
NOTE:

The E1 M/HDSL Unit is typically powered by the ac power module. Use the following procedures only if you want to use an optional dc power source.

▶ Procedure

To use the dc power cable:

1. Connect the green wire to a suitable earth ground.
2. Connect the orange wire to the +24 Vdc source.
3. Connect the white wire to the return.
4. Cut the black, red, and blue wires off at the outer insulation.
5. Plug the power connector into the 7986 Standalone Termination Unit.



+24 Vdc Power Supply Pinouts

Connecting to the Network

▶ Procedure

To connect your unit to the network:

1. Connect one end of the network cable into the rear panel DSL jack. Connect the other end to your DSL network interface.

   NOTES:

   A crossover cable (Pins 1, 2 to 4, 5) is required for connecting two 7986 Termination Units back-to-back.

   Do *not* use a flat VF network cable as this may severely degrade the performance of the termination unit. Use only Cat 5 twisted-pair network cable.

Connecting to a System Terminal

An optional system maintenance terminal may be attached to your Hotwire 7986 Standalone Termination Unit through the modular jack on the rear panel. The system maintenance terminal allows you to view the status of the unit, and change configuration options. The terminal must be a VT100-compatible terminal or a PC running terminal emulation software.

Connect the 9-pin end of the terminal cable into a COM port on your PC. Plug the other end into the modular jack on the rear panel. If your PC requires a 25-pin connector to the COM port, see Appendix C, *Cables and Pin Assignments*, for the correct cable pinouts.

Make sure the communication parameters on your PC or terminal are set to:

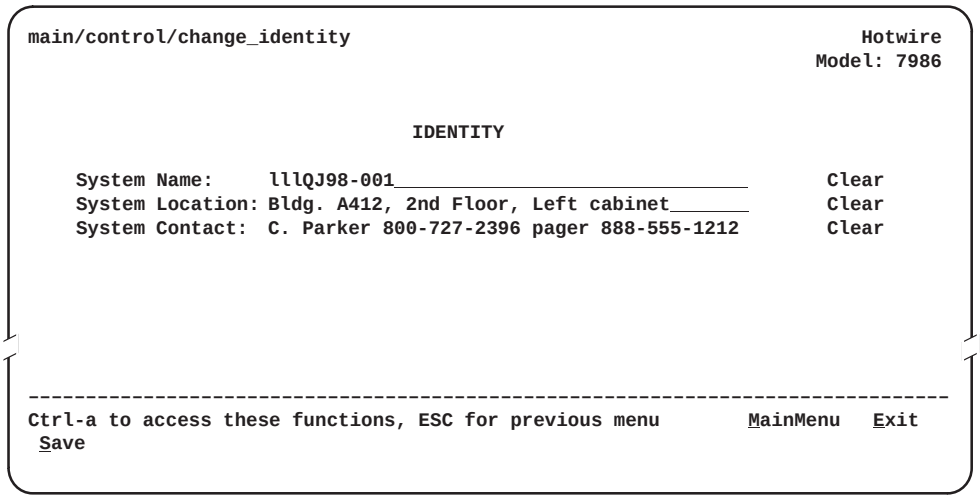
- 9600 baud
- 8 bit characters
- no parity
- 1 stop bit
- no flow control

Press Enter from your terminal or PC to activate the Main Menu for the attached unit. The system runs diagnostics and status checks. After a few moments, the Main Menu or Logon screen appears on your terminal.

Entering Identity Information

After accessing your unit for the first time, use the Change Identity screen to determine SNMP administrative system information that will be displayed on the Identity screen of the Status branch. To access the Identity screen, follow this menu selection sequence:

Main Menu → Control → Change Identity



The three System entry fields are alphanumeric and provide 128 characters for each field. The System entries appear on the Identity display as shown above. The SNMP System entry fields are:

- **System Name:** The general SNMP system name.
- **System Location:** The physical location of the SNMP-managed device.
- **System Contact:** Identification information, such as contact name, phone number, or mailing address.

Valid entry values are any printable ASCII character. ASCII printable characters include:

- Numeric 0–9
- Upper or lower case A–Z
- Space
- All ASCII symbols except the caret (^)

Select Clear to reset a field to a null value.

▶ Procedure

To enter Change Identity screen information:

1. Position the cursor in the System Name field. Enter a name unique in your network to identify the SNMP managed node (or unit).

   The maximum length of System Name is 128 characters.

2. Position the cursor in the System Location field. Enter the physical location of the unit.

   The maximum length of System Location is 128 characters.

3. Position the cursor in the System Contact field. Enter the name and contact information for the person responsible for the unit.

   The maximum length of System Contact is 128 characters.

4. Press Ctrl-a to switch to the screen function key area below the dotted line.

5. Select Save and press Enter.

Choosing a Configuration Mode

You can make configuration changes either through a VT100-compatible terminal and the unit's Configuration menus or by manually changing switches on the board. The unit comes defaulted to allow settings to be made through the Configuration menus.

Configuring the Unit Using the Configuration Menus

Use the Configuration menu to select, display, or change configuration option settings.

Configuration Options

NOTE:

The 7986 Standalone Termination Unit is pre-configured as an NTU. If you are using this unit as an NTU, the following configuration options may not need to be performed.

The 7986 Standalone Termination Unit is shipped with factory settings in the Default Factory configuration area. You can find default information by:

- Referring to Appendix A, *Configuration Option Tables*.
- Accessing the Configuration branch of the 7986 Standalone Termination Unit menu.

The 7986 Standalone Termination Unit has two sets of configuration option settings. The Current Configuration matches the Default Factory Configuration until modified and saved by the user.

Configuration Option Area	Configuration Option Set
Current Configuration	The 7986 Standalone Termination Unit's active set of configuration options.
Default Factory Configuration	A read-only configuration area containing the factory default configuration options.

If the factory default settings do not support your network's configuration, you can customize the configuration options for your application.

Configuring the Unit Using the Internal Switches

Use internal Switchpacks S1 and S2 to manually configure the unit. Use Figure 3-1 to locate Switchpacks S1 and S2.

⚠ HANDLING PRECAUTIONS FOR STATIC-SENSITIVE DEVICES

This product is designed to protect sensitive components from damage due to electrostatic discharge (ESD) during normal operation. When performing installation procedures, however, take proper static control precautions to prevent damage to equipment. If you are not sure of the proper static control precautions, contact your nearest sales or service representative.

▶ Procedure

To configure the unit using internal Switchpacks S1 and S2:

1. Power down the unit and remove the enclosure cover, exposing the circuit board.
2. Locate Switchpack S1 using Figure 3-1.
3. Set Switch 1 on Switchpack S1 to ON to enable Switchpacks 1 and 2.
4. After you enable the switchpacks, you must set the switches to your desired configuration. Refer to Figure 3-1 and Table 3-1.
5. Replace and secure the cover.
6. Power up the board to reset and enable the new configuration.

Switchpack Locations

Use Figure 3-1 to locate Switchpacks S1 and S2.

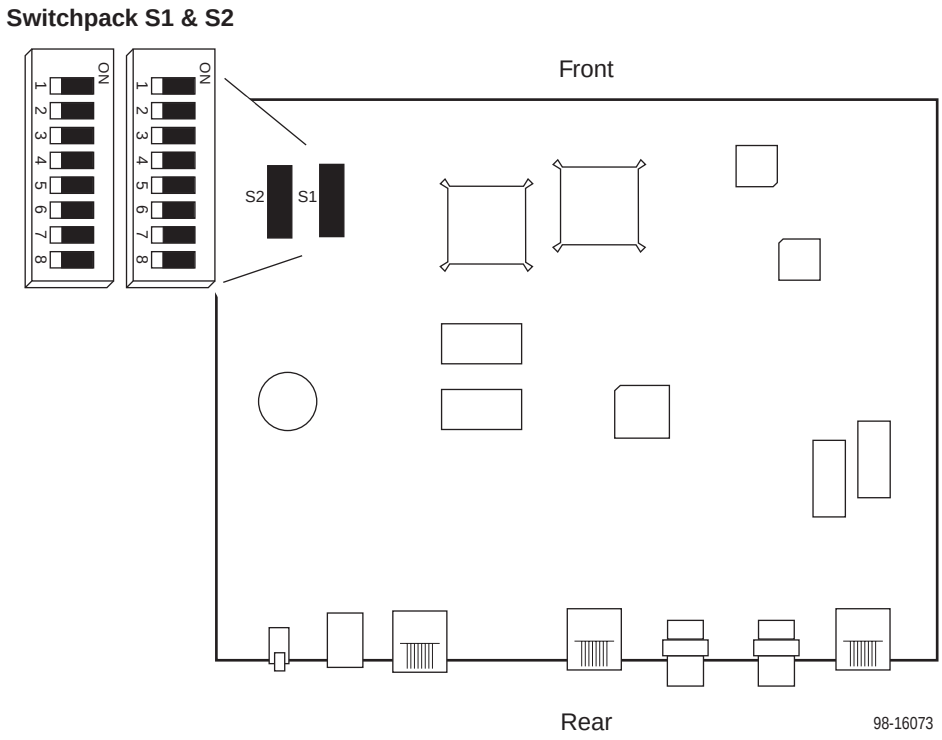


Figure 3-1. Hotwire 7986 Standalone Termination Unit Switchpack Locations

Switchpack Definitions

Manually change configuration options by moving Switchpack S1 DIP switches on the card. Table 3-1 lists Switchpack S1 definitions.

Table 3-1. Switchpack S1 Definitions

Switch # . . .	**Allows you to . . .** *Default in **Bold***
1	Enable or disable Switchpacks S1 and S2. **OFF = Switchpacks Disabled** ON = Switchpacks Enabled
2	Control line termination. **OFF = 120 Ohm** ON = 75 Ohm
3	Select the unit's primary timing source. Only valid for units configured as LTU. **OFF = Internal Clock** ON = External Clock
4	Control the unit's E1 line coding. **OFF = HDB3** ON = AMI
5	Not used
6	Enable CRC-4 monitoring. **OFF = Enable CRC-4** ON = Disable CRC-4 monitoring
7	Control whether Channel 16 contains signaling information or data. **OFF = Channel 16 is used for signaling** ON = Channel 16 is used for data
8	Not used

Table 3-2 lists Switchpack S2 definitions.

Table 3-2. Switchpack S2 Definitions

Switch # . . .	**Allows you to . . .** *Default in **Bold***
1	Control whether the unit is an LTU or an NTU. **OFF = NTU** ON = LTU
2	Control enabling and disabling of the AutoRate capability. Only valid for units configured as LTU. **OFF = AutoRate Disabled** ON = AutoRate Enabled
3, 4, 5	Select one of eight preset DSL line rates (refer to Table 3-3). **All OFF = 2064**
6, 7	Not used
8	**Emergency Use Only** – The 7986 has two banks of flash memory used to hold executable firmware. This switch allows you to switch between the two versions of firmware. This switch is independent from the position of Switch 1 on Switchpack S1 (switchpack enable/disable). **OFF = Current Firmware** ON = Previous Firmware

Use Table 3-3 to set the DSL Line Rate. Defaults are shown in bold.

Table 3-3. DSL Line Rate, Switches 3 – 5 on Switchpack S2

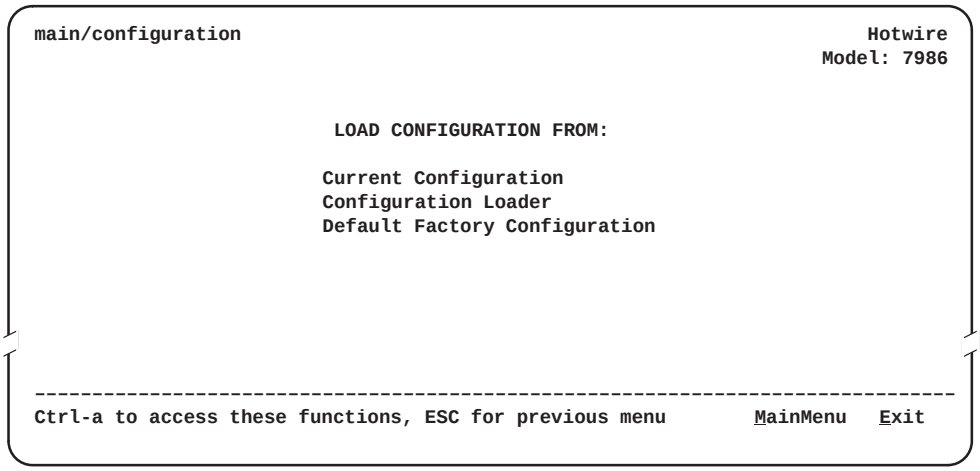
Switch Position				
5	**4**	**3**		**DSL Line Rate**
OFF	ON	ON		400 kbps
ON	OFF	OFF		528 kbps
ON	OFF	ON		784 kbps
ON	ON	OFF		1040 kbps
ON	ON	ON		1552 kbps
OFF	**OFF**	**OFF**		**2064 kbps**

Accessing and Displaying Configuration Options

To display configuration options, you must first load a configuration into the edit area.

To load a configuration option set into the configuration edit area, follow this menu selection sequence:

Main Menu → Configuration (Load Configuration From)



Make a selection by placing the cursor at your choice and pressing Enter.

If you select . . .	Then . . .
Current Configuration	The selected configuration option set is loaded and the Configuration Edit/Display menu screen appears.
Default Factory Configuration	The selected configuration option set is loaded and the Configuration Edit/Display menu screen appears.
Configuration Loader	The Configuration Loader screen is displayed allowing you to upload or download configurations from a TFTP server.

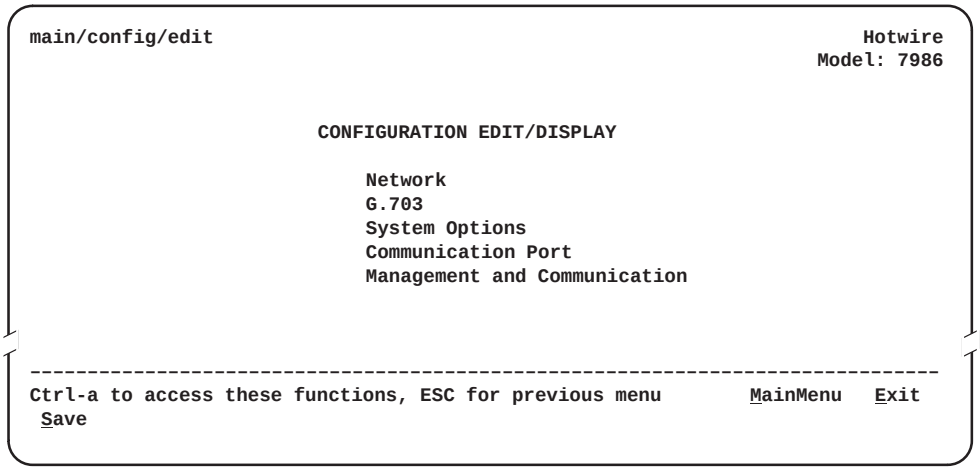
Configuration Edit/Display

The Configuration Edit/Display screen is displayed when the current, customer, or default configuration is loaded. To access the Configuration Edit/Display screen, follow this menu selection sequence:

Main Menu → Configuration → Current Configuration

– or –

Main Menu → Configuration → Default Factory Configuration



See Appendix A, *Configuration Option Tables*, for a list and explanation of the configuration options available.

Select . . .	To Access the . . .	To Configure the . . .
Network	Network Interface Options, Table A-1	DSL network interfaces on the unit.
G.703	G.703 Interface Options, Table A-2	G.703 interface.
System Options	System Options, Table A-3	General system options of the unit.
Communication Port	Communication Port Options, Table A-4	Unit's COM port options.
Management and Communication	■ Telnet Session Options, Table A-5 ■ Communication Protocol Options, Table A-6 ■ SNMP Traps Options, Table A-7 ■ General SNMP Management Options, Table A-8 ■ SNMP NMS Security Options, Table A-9	Management support of the unit through SNMP and Telnet.

Configuring AutoRate

The M/HDSL AutoRate function is controlled from the Network Interface Options screen and allows you to enable or disable AutoRate only from a unit configured as an LTU. To access the Network Interface screen, follow this menu selection sequence:

Main Menu → Configuration → Network

```
main/config/network                                              Hotwire
                                                               Model: 7986


                          NETWORK INTERFACE OPTIONS

                    Margin Threshold:                -3db
                    Excessive Error Rate Threshold:  1E-6
                    AutoRate                         Disable
                    DSL Line Rate                    528


                    Peer IP Address:                 111.255.255.000  Clear

    Circuit Identifier: _____________________________________________  Clear




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
 Save
```

▶ Procedure

The AutoRate option is defaulted to Disable. To enable AutoRate:

1. Position the cursor in the AutoRate field and press the spacebar.

   The AutoRate field toggles to Enable and the DSL Line Rate field displays.

2. Enter a DSL Line Rate and press Enter.

   Your payload rate is set to a default value of 1984. Use Table 3-5, Fixed Rate Payload Rates and DSL Line Rates, to set your DSL Line Rate and Payload Rate according to whether you are configured for Voice (signaling) or Data.

Table 3-4 provides the maximum payload rates achievable for each DSL line rate and the number of time slots required to achieve that payload rate depending on whether you are using signaling (time slots 0 and 16) or data only (time slot 0).

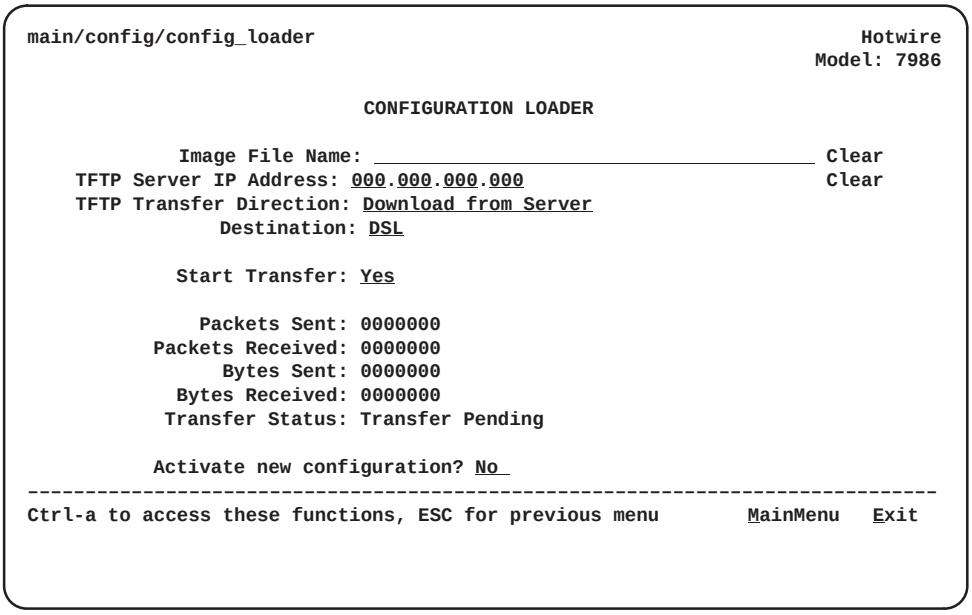
Table 3-4. Fixed Rate Payload Rates and DSL Line Rates

	Voice Mode (G.703 to G.703)		Data Mode (G.703 to G.703)		Data Mode (G.703 to EIA-530)	
DSL Line Rate (kbps)	**Maximum Payload Rate (kbps)**	**Time slots**	**Maximum Payload Rate (kbps)**	**Time slots**	**Maximum Payload Rate (kbps)**	**Time slots**
2064	1920	30	1984	31	1984	31
1552	1408	22	1472	23	1536	24
1040	896	14	960	15	1024	16
784	640	10	704	11	768	12
528	384	6	448	7	512	8
400	256	4	320	5	384	6

Configuration Loader

The Configuration Loader screen allows you to upload configurations to and download configurations from a TFTP server. To access the Configuration Loader screen, follow this menu selection sequence:

Main Menu → Configuration → Configuration Loader



▶ Procedure

To upload or download a configuration:

1. Position the cursor in the Image File Name field. Type the name of the file to be downloaded, or the name to be used for the file to be uploaded.

   The file name may be a regular path name expression of directory names separated by a forward slash (/) ending with the file name. The total path name length can be up to 128 characters.

   DOS machine: If the TFTP server is hosted by a DOS machine, then directory and file names must consist of eight or less characters with an optional suffix of up to three characters. The system will automatically upload the configuration file and create directories and file names as needed.

   UNIX machine: If your server is hosted by a UNIX machine, the configuration file you name must already exist. It will not be created on the UNIX system by the TFTP server. It is critical that you work with your system administrator to plan the naming conventions for directories, filenames, and permissions so that anyone using the system has read and write permissions.

2. Position the cursor in the TFTP Server IP Address field. Enter the TFTP server IP address.
3. Position the cursor in the Destination field. Use the spacebar to select a network destination for the TFTP server. Select DSL if the TFTP server destination is the DSL link or COM if the TFTP destination is the COM port.
4. Position the cursor in the TFTP Transfer Direction field. Use the spacebar to select Download from Server or Upload to Server.
5. Position the cursor at the Start Transfer field. Use the spacebar to select Yes. Press Enter.

   When the data transfer is complete, the Transfer Status field changes to **`Completed successfully`**.
6. Position the cursor at the Activate New Configuration field and select Yes to activate a new downloaded configuration. Press Enter.

NOTE:

The configuration options DSL Mode and Telnet Session are **not** changed when a new configuration is loaded. You must change these settings with the appropriate configuration menus after the new configuration is activated. See Table A-3, System Options, and Table A-5, Telnet Session Options, in Appendix A, *Configuration Option Tables*.

Saving Configuration Options

When changes are made to the configuration options through the Configuration Edit/Display branch, the changes must be saved to take effect. Use the Save key or Save Configuration screen.

▶ Procedure

To save configuration options changes:

1. Press Ctrl-a to switch to the screen function key area below the dotted line.
2. Select Save and press Enter.

NOTE:

When Exit is selected before Save, or Save has been selected from any menu in the Configuration/Edit branch, a Save Configuration screen appears requiring a Yes or No response.

```
main/config/saveprompt                                          Hotwire
                                                              Model: 7986


                              SAVE CONFIGURATION

                              Save Changes? No

                                  WARNING:

                    An answer of "yes" will cause the system
                    to reset as if it had been powered off and on!


--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit

Command Complete
```

If the Telnet Session configuration option is changed, a message displays on the Save Configuration screen warning that an answer of Yes will cause the Telnet session to disconnect. Do not answer Yes unless you are prepared to disconnect.

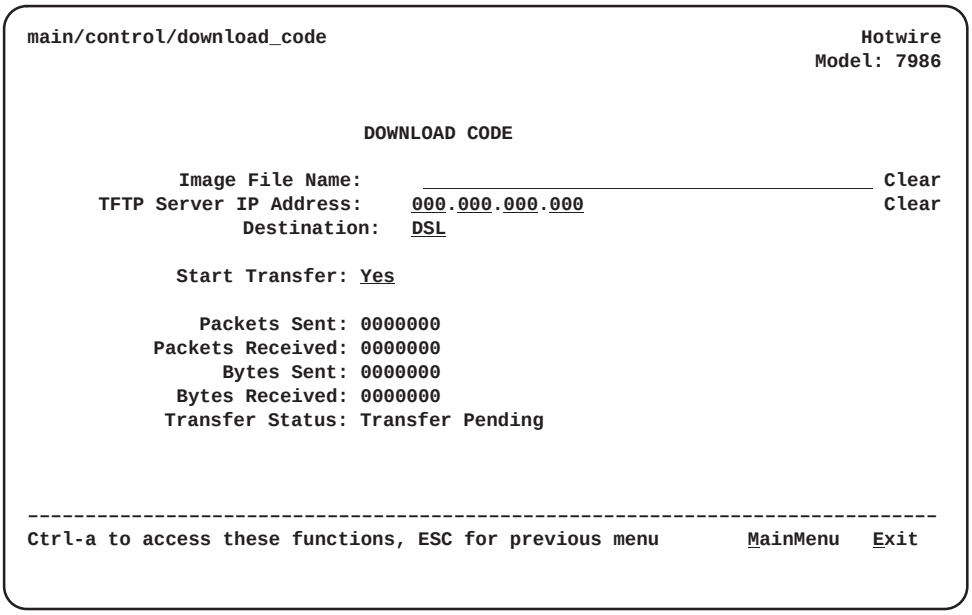
If the DSL Mode configuration option is changed, a message displays on the Save Configuration screen warning that an answer of Yes will cause the system to reset. Do not answer Yes unless you are prepared to reset.

If you select . . .	Then . . .
Yes	The configuration is saved.
No	The Main Menu appears and changes are not saved.

Download Code

The Download Code screen allows you to download firmware from a TFTP server. To access the Download Code screen, follow this menu selection sequence:

Main Menu → Control → Download Code



▶ Procedure

To download firmware:

1. Position the cursor in the Image File Name field. Type the name of the file to be downloaded.

   The file name may be a regular path name expression of directory names separated by a forward slash (/) ending with the file name. The total path name length can be up to 128 characters.

2. Position the cursor in the TFTP Server IP Address field. Enter the TFTP server IP address.

3. Position the cursor in the Destination field. Use the spacebar to select a network destination for the TFTP server. Select DSL if the TFTP server destination is the DSL link or COM if the TFTP destination is the COM port.

4. Position the cursor at the Start Transfer field. Use the spacebar to select Yes. Press Enter.

   When the data transfer is complete, the Transfer Status field changes to **`Completed successfully`**.

5. Press the Escape key to return to the Control menu. Select Apply Download.

6. On the Apply Download screen, select Yes to reset the card and activate the code.

Monitoring the Unit

4

What to Monitor

This chapter presents information on how to access and monitor Hotwire 7986 Standalone Termination Units on the E1 network. You can monitor 7986 Standalone Termination Unit operations by viewing:

- System and Test Status screens
- Highest priority Health and Status messages on the last line of all screens
- Network Error Statistics screen
- Network Performance Statistics screen
- G.703 Statistics screen
- Display LEDs screen or LEDs on the 7986 Standalone Termination Unit front panel

Viewing System and Test Status

To view System and Test Status information, follow this menu selection sequence:

Main Menu → *Status* → *System and Test Status*

```
main/status/system                                                    Hotwire
                                                                   Model: 7986

                            SYSTEM AND TEST STATUS                 Page 1 of 1

HEALTH AND STATUS            SELF-TEST RESULTS        TEST STATUS
--------------------------------------------------------------------------------
LOS at Net, Pt 1             Device Failed                No Test Active









--------------------------------------------------------------------------------
                                  ESC for previous menu       MainMenu   Exit
PgUp    PgDn
```

The System and Test Status screen has three sections:

- **Health and Status** – Displays messages in priority order (highest to lowest). Refer to Table 4-1, Health and Status Messages.
- **Self-Test Results** – Results of the Diagnostic test run on the device itself. Refer to Table 4-2, Self-Test Results Messages.
- **Test Status** – Currently active tests. Refer to Table 4-3, Test Status Messages.

Health and Status

The following messages can appear in the first column of the System and Test Status screen. The highest priority Health and Status message also appears on all ATI screens on the bottom right.

Table 4-1. Health and Status Messages (1 of 2)

Message	What Message Indicates	What To Do
System Operational	There are no problems detected.	
LOS at Net, Pt 1	An LOS (Loss Of Signal) condition has been detected on the network interface. No signal is being received on Port 1, possibly due to a local network problem.	1. Verify that the network cable is securely attached at both ends. 2. Contact network provider.
OOF at Net, Pt 1	An OOF (Out Of Frame) condition has been detected.	1. Check the Transmit Clock Source configuration options. Do not set both the local and remote unit to Internal, External, or Loop timing. 2. Contact network provider.
LOF at G.703, Pt 1	An LOF (Loss Of Frame) condition has been detected on the G.703 interface.	1. Verify that the network cable is securely attached at both ends. 2. Contact network provider.
AIS at G.703, Pt 1	An Alarm Indication Signal (AIS) is being received by the G.703 interface.	1. Check the Transmit Clock Source configuration options. Do not set both the local and remote unit to Internal, External, or Loop timing. 2. Contact network provider.
EER at Net, Pt 1	An EER (Excessive Error Rate) condition has been detected on the network interface at Port 1. The condition is cleared when the error rate falls below the threshold value currently configured.	Contact network provider.
EER at G.703, Pt 1	An EER (Excessive Error Rate) condition has been detected on the G.703 interface.	Contact network provider.
RAI (Remote Alarm Indication) at G.703 interface, Pt 1	An Remote Alarm Indication signal is being received by the G.703 interface.	Contact network provider.
Net Margin Threshold, Pt 1	The signal-to-noise margin has exceeded the configured threshold.	Contact network provider.

Table 4-1. Health and Status Messages (2 of 2)

Message	What Message Indicates	What To Do
Fallback Rate, Pt 1	The LTU, set to AutoRate enable, synchronized at a lower rate when the line was restored after an LOS.	Reset AutoRate. AutoRate is designed to find the best rate possible for your DSL loop conditions. After the DSL loop is up units should be run in fixed rate.
Primary Clock Failed (G.703 Pt 1)	A failure has occurred in the primary clock source configured from the Network, G.703, or from the card internal clock.	1. Verify that the network cable is securely attached at both ends. 2. Contact network provider.
DeviceFailed *yyyyyyyy*	An internal error has been detected by the operating software. *yyyyyyyy* indicates the 8-digit hexadecimal failure code.	1. Provide the 8-digit failure code shown (*yyyyyyyy*) to your service representative. 2. Reset the 7986 Standalone Termination Unit to clear the condition and message.
Download Failed	A firmware download was interrupted.	Repeat the download.
Net Com Link Down	The Network communication link is down. Communications between the management system and the LTU/NTU is not possible.	1. Verify that the network cable is securely attached at both ends. 2. Verify the link protocol for the COM port is configured correctly.
Mismatch Rate, Pt 1	The LTU, in fixed rate, is attempting to communicate at a faster rate than the NTU can handle.	1. Verify endpoint is not a 1 Mbps product. 2. Upgrade remote unit to a 2 Mbps or reconfigure the LTU for fixed rate at a lower rate.
NTU TS16 Not Supported	The LTU is configured for TS16 signaling and the NTU is not configured to support TS16 signaling.	1. Verify endpoint is a G.703 product. EIA-530A products do not support signaling. 2. Replace endpoint or reconfigure TS16 to data.

Self-Test Results

The results of the last power-up or reset self-test appear in the middle column of the System and Test Status screen.

Table 4-2. Self-Test Results Messages

Message	What Message Indicates	What To Do
CPU Failed	The CPU failed internal testing.	1. Reset the unit and try again. 2. Call your service representative for assistance.
DeviceFailed	One or more of the Unit's integrated circuit chips failed device-level testing.	
G.703 Failed, Pt 1	The Unit failed to loop data on the G.703 on Port 1.	1. Reset the unit and try again. 2. Call your service representative for assistance.
Memory Failed	The Model 7986 Standalone Termination Unit failed memory verification.	
Failure *xxxxxxxx*	An internal failure occurred. (*xxxxxxxx* represents an 8-digit hexadecimal failure code for use by service personnel.)	Record the failure code and contact your service representative.
Passed	No errors were detected.	

Test Status

The Test Status messages in the following table appear in the right column of the System and Test Status screen.

Table 4-3. Test Status Messages

Test Status Message	Meaning
No Test Active	No tests are currently running.
LLB Test Active, Pt 1	A network Line Loopback test is active on Port 1.
PLB Test Active, Pt 1	A Payload Loopback test is active on Port 1.
DTE Test Active, Pt 1	A Data Terminal Loopback test is active on Port 1.
RLB Test Active, Pt 1	A Repeater Loopback test is active on Port 1.
511 Test Active, Pt 1	A 511 Test and Monitor is active on the DSL Port 1 network interface.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the front panel to light.

For further information on testing, refer to Chapter 5, *Testing*.

Viewing Network Error Statistics

The Model 7986 Standalone Termination Unit maintains error statistics on the network DSL interface for port 1. Statistics are maintained for up to 96 15-minute intervals (24 hours).

To view the Network Error Statistics, follow this menu selection sequence:

Main Menu → Status → Performance → Network Error Statistics

```
main/status/performance/net_error                                    Hotwire
                                                                   Model: 7986
                          NETWORK ERROR STATISTICS

    Current Interval Timer: 002                      Error Events Counter: 0034
-------------------------------------------------------------------------------
               ---ES---        ---SES---        --FEBE--          -Complete-
               Near Far        Near Far         Near Far          Near Far
  Current Int: 000  000        000  000         000  000          Yes  No
  Interval 01  000  000        000  000         000  000          Yes  Yes
  Interval 02  000  000        000  000         000  000          Yes  Yes
  Interval 03  000  000        000  000         000  000          Yes  Yes
  Interval 04  000  000        000  000         000  000          Yes  Yes
  Interval 05  000  000        000  000         000  000          Yes  Yes
  Interval 06  000  000        000  000         000  000          Yes  Yes
  Interval 07  000  000        000  000         000  000          Yes  Yes

Worst Interval: 24   09         14   08          18   18
Near Tot(valid):  00010           00000            00000
 Far Tot(valid):  00010           00000            00000
-------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu         MainMenu   Exit
 PgUp     PgDn    ClrNear   ClrFar
```

Select PgUp or PgDn to view more statistics, Select ClrNear or ClrFar to clear the near- and far-end statistics to zero.

Network Error Statistics are collected for:

- **ES (Errored Seconds):** Seconds during which one or more ESF error event occurred.
- **SES (Severely Errored Seconds):** Seconds during which more than 320 cyclic redundancy check (CRC) error events or at least one Out of Frame (OOF) event occurred.
- **FEBE (Far-End Block Errors):** Errors reported by the remote equipment.
- **Complete**: Whether the interval register contains data for a complete 900-second interval.

Use the virtual function keys to page through the intervals and clear statistics.

This Field . . .	**Contains . . .**
Current Interval Timer	The number of seconds which have elapsed in the current 15-minute interval. Maximum value is 900 seconds (15 minutes). This counter resets every 15 minutes.
Error Events Counter	A running total of CRC errors. Range 0 – 65535. This counter resets when the near-end data is cleared.
Current Interval	Performance data for the current 15 minutes.
Interval *xx*	Historical performance data for up to 96 15-minute intervals (24 hours) where the value of *xx* is from 01 to 96.
Worst Interval	The number of the interval with the worst (highest) performance data for both the near- and far-end statistics. If two or more intervals are equal, the oldest interval is displayed.
Near and Far TOT	A 24-hour running total of the near- and far-end performance statistics.

Viewing Network Performance Statistics

Network performance statistics allow you to monitor the current status of the network DSL operations. Performance statistics can assist you in determining the duration of specific conditions and provide a historical context for problem detection and analysis. Statistics are maintained for up to 96 15-minute intervals (24 hours).

To view the Network Performance Statistics, follow this menu selection sequence:

Main Menu → Status → Performance → Network Performance Statistics

```
main/status/performance/net_perf                                    Hotwire
                                                                  Model: 7986
                    NETWORK PERFORMANCE STATISTICS
                                                      Payload Rate: 1984
   Current Interval Timer: 2                         DSL Line Rate: 2064 kbps
-------------------------------------------------------------------------------
              --Mrgn--        --XmtPw-        --RxGn--          -Complete-
              Near Far        Near Far        Near Far          Near Far
  Current Int: +02  +01        +03  +03        +02  +02          Yes  Yes
  Interval 01  +02             +03             +02               Yes  No
  Interval 02  +02  +01        +03  +03        +02  +02          Yes  Yes
  Interval 03  +02  +01        +03  +03        +02  +02          Yes  Yes
  Interval 04  +02  +01        +03  +03        +02  +02          Yes  Yes
  Interval 05  +02  +01        +03  +03        +02  +02          Yes  Yes
  Interval 06  +02  +01        +03  +03        +02  +02          Yes  Yes
  Interval 07  +02  +01        +03  +03        +02  +02          Yes  Yes




-------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu         MainMenu   Exit
 PgUp     PgDn    ClrNear   ClrFar
```

Select PgUp or PgDn to view more statistics, Select ClrNear or ClrFar to clear the near- and far-end statistics to zero.

Network Performance Statistics are collected for:

- **Mrgn:** Margin, the signal-to-noise ratio (SNR) less an SNR reference value.
- **XmtPw:** The transmit power level.
- **RxGn:** The receiver gain level.
- **Complete:** Whether the interval register contains data for a complete 900-second interval.

This Field . . .	Contains . . .
Current Interval Timer	The number of seconds which have elapsed in the current 15-minute interval. Maximum value is 900 seconds (15 minutes). This counter resets every 15 minutes.
Payload Rate	The Payload Rate across the DSL interface.
DSL Line Rate	The rate of the DSL line. The Line Rate can be 144 kbps, 272 kbps, 400 kbps, 528 kbps, 784 kbps, 1040 kbps, 1552 kbps, or 2064 kbps.
Current Interval	Performance data for the current 15 minutes.
Interval *xx*	Historical performance data for up to 96 15-minute intervals (24 hours) where the value of *xx* is from 01 to 96.

Viewing G.703 Performance Statistics

G.703 performance statistics allow you to monitor the current status of the network DSL operations. Performance statistics can assist you in determining the duration of specific conditions and provide a historical context for problem detection and analysis. Statistics are maintained for up to 96 15-minute intervals (24 hours).

To view the Network Performance Statistics, follow this menu selection sequence:

Main Menu → Status → Performance → Network Performance Statistics

```
main/status/performance/G.703                                        Hotwire
                                                                   Model: 7986
                      G.703 PERFORMANCE STATISTICS

    Current Interval Timer: 2                      Error Events Counter: 0000
-------------------------------------------------------------------------------
               --ES--    --UAS--    --SES--     --BES--   --LOFS--   -Status-

Current Int:    000       000        000         000        000        Y
Interval 01     000       000        000         000        000        none
Interval 02     000       000        000         000        000        none
Interval 03     000       000        000         000        000        none
Interval 04     000       000        000         000        000        none
Interval 05     000       000        000         000        000        none
Interval 06     000       000        000         000        000        none
Interval 07     000       000        000         000        000        none

Worst Interval: 24         14         14          09         18
Tot (valid 96):00010      00000      00000       00000      002

-------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu          MainMenu   Exit
 PgUp     PgDn    ClrStats
```

Select PgUp or PgDn to view the next or previous seven intervals, select ClrStats to clear all statistics to zero.

G.703 Performance Statistics are collected for:

- **ES (Errored Seconds):** Seconds during which one or more ESF error event occurred.
- **UAS (Unavailable Seconds):** Seconds during which service is unavailable. UAS is received at the start of 10 consecutive SES and cleared at the start of 10 seconds with no-SES.
- **BES (Bursty Errored Seconds):** Contains the number of bursty errored seconds for the current interval. A bursty errored second is any second with more than one but less than 805 CRC errors.
- **SES (Severely Errored Seconds):** Seconds during which more than 805 cyclic redundancy check (CRC) error events, more than 16 FAS errors, or at least one Out of Frame (OOF) event occurred.
- **LOFS (Loss of Frame Seconds):** Contains the number of seconds that contain an LOF.

- **Status:** Contains the contents of the status events register. The status events register maintains a history of specific events that have occurred during an interval. Values include:
  - Y – Remote alarm indication signal received at the G.703 interface
  - L – Loss of signal detected at the G.703 interface
  - E – Excessive error rate threshold exceeded
  - F – Frame synchronization bit error detected
  - V – Line code violation detected
  - None – No significant events have occurred

This Field . . .	Contains . . .
Current Interval Timer	The number of seconds which have elapsed in the current 15-minute interval. Maximum value is 900 seconds (15 minutes). This counter resets every 15 minutes.
Current Interval	Performance data for the current 15 minutes.
Interval *xx*	Historical performance data for up to 96 15-minute intervals (24 hours) where the value of *xx* is from 01 to 96.
Error Events Counter	A running total of CRC and OOF events. Total range = 0–65535. Counter resets when the statistics are cleared.

Viewing 7986 Standalone Termination Unit LEDs

The 7986 Standalone Termination Unit LEDs can be viewed on the Display LEDs Status screen. This ATI status screen is available locally and remotely.

The three groups of LEDs are:

- **General** LEDs display the status of the unit
- **G.703** LEDs provide the status of the G.703 interface
- **DSL Loop** LEDs display the activity on the DSL network

To view the LED status screen, follow this menu selection sequence:

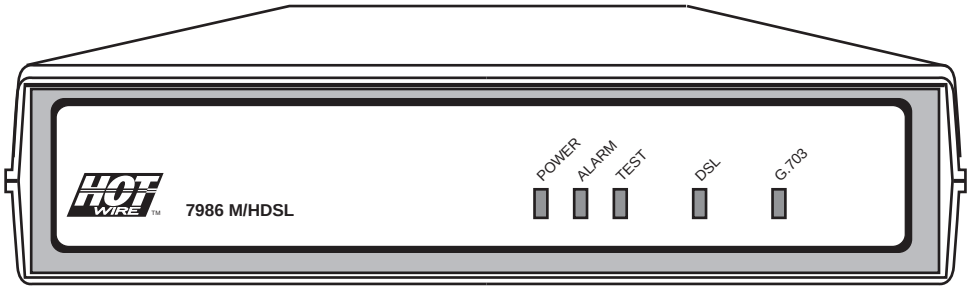
Main Menu → Status → Display LEDs

```
main/status/leds                                                    Hotwire
                                                                  Model: 7986


                              DISPLAY LEDs

                  GENERAL          G.703               DSL LOOP
-------------------------------------------------------------------------------
                  ALRM:Off         P1:Link Up          P1:Lnk Up
                  TEST On


-------------------------------------------------------------------------------
                                  ESC for previous menu       MainMenu   Exit
```

The LED status display screen is updated every 5 seconds. For information about the meaning of 7986 Standalone Termination Unit LEDs, see *7986 Standalone Termination Unit LEDs* on page 4-14.

Hotwire 7986 Standalone Termination Unit LEDs

The following table contains a description of the LEDs on the 7986 Standalone Termination Unit front panel.



98-16087

Type	LED	LED is . . .	Indicating . . .
General	POWER	Green	Unit has power.
		Off	No power to the Unit.
		Green, Flashing	Unit is in minimum mode and a download is required.
	ALARM	Red	Device failure, or Power-On Self-Test (POST) is not complete.
		Off	Self-test passed.
	TEST	Amber	Loopback test or 511 test pattern in progress.
		Amber, flashing	Self-test in progress.
		Off	No tests.
DSL	DSL	Green	DSL link is up.
		Amber	DSL training in progress.
		Amber, flashing	An OOF condition exists.
		Off	The DSL Link is down.
G.703	DTE	Green	Recoverable signal present on the G.703 network.
		Amber	Remote Alarm Indication (RAI) present.
		Amber, flashing	OOF condition exists.
		Off	The G.703 LINK is down.

Testing

5

Accessing the Test Menu

From the Test menu, you can run network tests, data port tests, and a front panel lamp test.

To access the Test menu, follow this menu selection sequence:

Main Menu → Test

```
main/test                                                          Hotwire
                                                                Model: 7986


                                      TEST

                                Network & G.703 Tests
                                Device Tests

                                Abort All Tests




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu        MainMenu   Exit
```

Select . . .	To . . .
Network and G.703 Tests	Start and stop tests on the G.703 network interface.
Device Tests	Start and stop lamp test.
Abort All Tests	To abort all current tests excluding G.703 and Network-initiated loopback tests. An aborted test may continue to run for a few seconds as the abort command is sent to the remote end and processed.

Running Network Tests

Network tests require the participation of your network service provider. To access the Network Tests screen, follow this menu selection sequence:

Main Menu → Test → Network & G.703 Tests

```
main/test/network_G.703
Hotwire
                                                                  Model: 7986


                              NETWORK & G.703 TESTS

Test                          Command  Status     Results
-------------------------------------------------------------------------------
Local Loopbacks
  Line Loopback:              Start    Inactive   00:00:00
  Repeater Loopback:          Start    Inactive   00:00:00
  DTE Loopback:               Start    Inactive   00:00:00

Remote Loopbacks
  Send Line Loopback: Down    Send     Inactive   00:00:00

Pattern Tests
  Send and Monitor 511        Stop     Active     hh:mm:ss - Errors 99999+

-------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu        MainMenu   Exit
 ResetMon
```

Use the **Command** column to start or stop a test. When the **Status** column shows that a test is Inactive, Start is displayed; when a test is Active, Stop is displayed. Position the cursor at the desired Start or Stop command and press Enter.

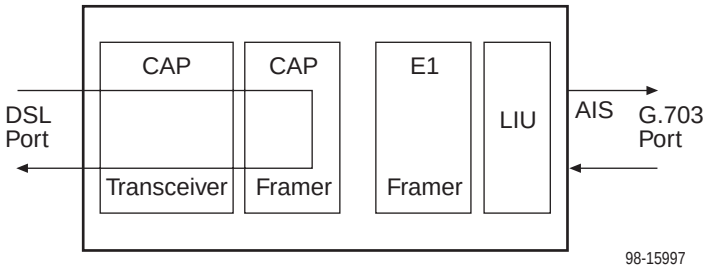
Selecting a Stop command on the Network Tests screen or Abort All Tests from the Test menu will not disrupt a network-initiated loopback.

The **Results** column displays the test duration.

When the Send and Monitor 511 test is active, ResetMon is available to reset the error counter to zero.

Line Loopback

Line Loopback (LLB) loops the received signal on the network interface back to the network without change.



▶ Procedure

To run a Line Loopback:

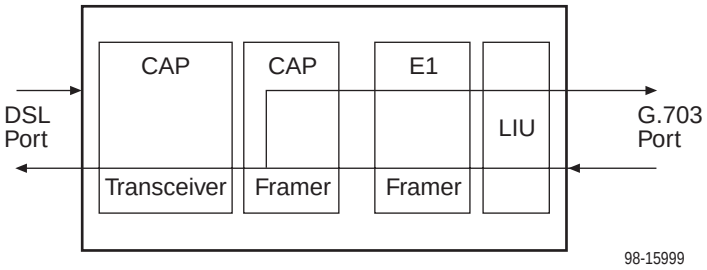
1. Position the cursor at the Start command next to Line Loopback on the Network Tests screen.
2. Press Enter.

   The Start command is changed to Stop.
3. To manually stop the test, verify that the cursor is positioned at the Stop command.
4. Press Enter.

Line Loopback cannot be started when a Repeater Loopback, DTE Loopback, Remote DCLB, or network-initiated Line Loopback is in progress.

Repeater Loopback

Repeater Loopback (RLB) loops the signal being sent from the data port back to the data port and to the network interface.



▶ Procedure

To run a Repeater Loopback:

1. Position the cursor at the Start command next to Repeater Loopback on the Network Tests screen.
2. Press Enter.

   The Start command is changed to Stop.
3. To manually stop the test, verify that the cursor is positioned at the Stop command.
4. Press Enter.

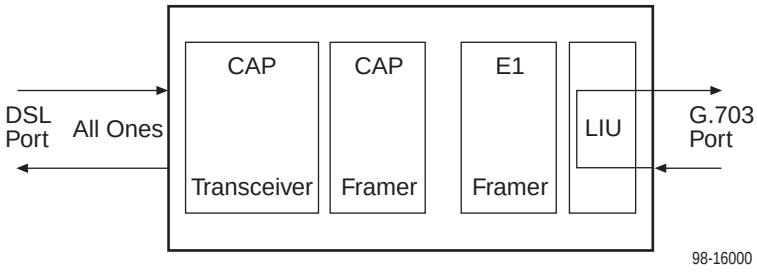
A Repeater loopback cannot be started when any other loopback test is in progress.

NOTE:

Activating the Repeater Loopback test causes the EOC to be lost to the remote unit.

DTE Loopback

DTE Loopback loops the G.703 signal back to itself before the signal is sent to the Framer.



▶ Procedure

To run a DTE Loopback:

1. Position the cursor at the Start command next to DTE Loopback on the Network Tests screen.
2. Press Enter.

   The Start command is changed to Stop.
3. To manually stop the test, verify that the cursor is positioned at the Stop command.
4. Press Enter.

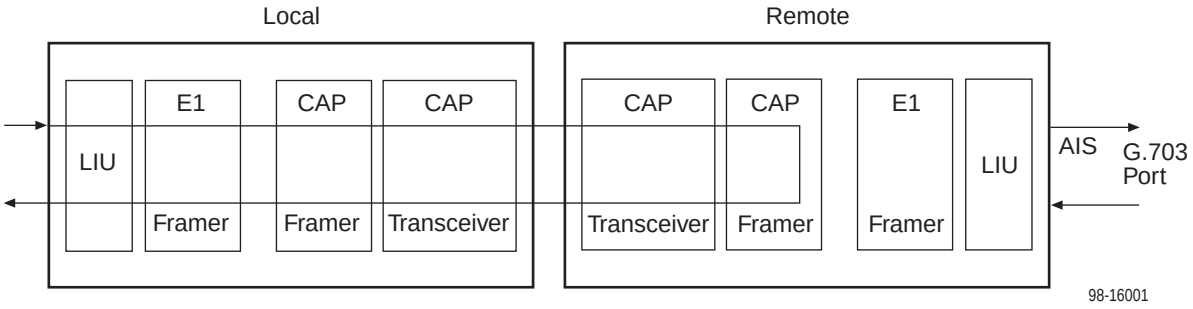
A DTE Loopback cannot be started when any other loopback test is in progress.

NOTE:

Activating the DTE Loopback test causes the EOC to be lost to the remote unit.

Send Remote Line Loopback

The LTU initiates the test by sending a line loopback up or down command to the remote unit for 10 seconds. When the remote unit detects the loopback up command, it puts itself in line loopback and lights the front panel test LED. The remote unit remains in loopback until it receives a loopback down command. The send line loopback tests both units. External equipment can be used to verify the link.



▶ Procedure

To run a Remote Send Line Loopback:

1. Position the cursor at the Up or Down selection next to Send Line Loopback on the Network Tests screen.
2. Press the spacebar to select either Up or Down.
3. Position the cursor at the Send command next to Up or Down selection.
4. Press Enter.

   The loopback stops automatically after 10 seconds. You cannot stop the test manually.

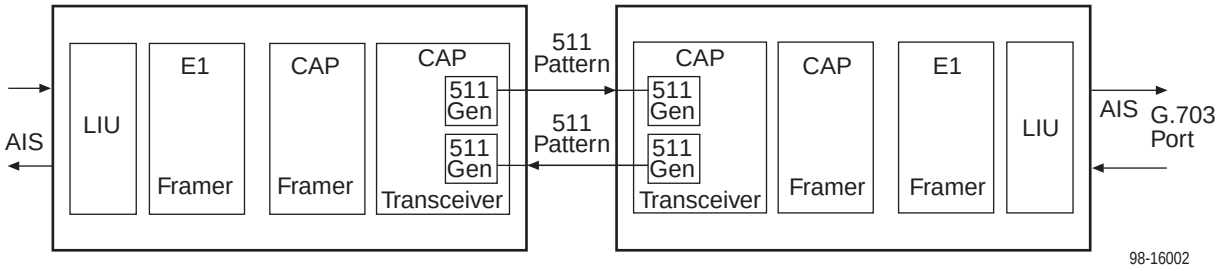
The Send Remote Line Loopback cannot be started when any other loopback or a Send and Monitor 511 test is active on the network interface.

Send and Monitor 511

The LTU initiates the test by sending a command to the remote unit to send a 511 test pattern. When the remote unit detects the command, it sends a 511 pattern and lights the front panel test LED. Each unit will send and monitor the 511 pattern. The duration and results of the test are displayed on the Network Test screen of each unit.

NOTE:

The send and monitor test is not a loopback test. Each unit independently sends and monitors a 511 pattern.



▶ Procedure

To run a Send and Monitor 511 test:

1. Position the cursor at the Start command next to Send and Monitor 511 on the Network Tests screen.
2. Press Enter.

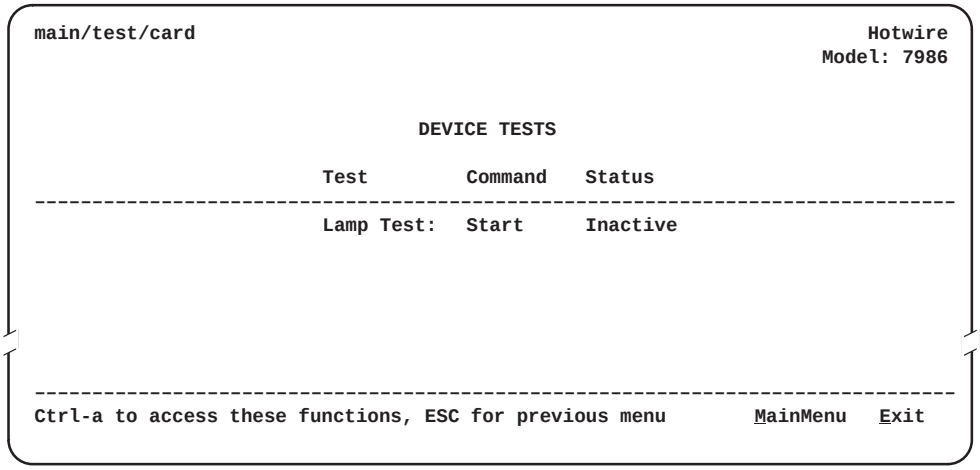
   The Start command is changed to Stop.
3. To manually stop the test, verify that the cursor is positioned at the Stop command.
4. Press Enter.

When a Send and Monitor 511 test is active, a count of bit errors is displayed next to the test duration, and the ResetMon virtual function key is available for use. Type **r** or **R** or select the ResetMon virtual function key to reset the error count.

Device Tests

The Device Tests branch is used to access the only card-level test, the Lamp Test. To access the Device Tests screen, follow this menu selection sequence:

Main Menu → Test → Device Tests



Lamp Test

The Lamp test determines whether all LEDs are lighting and functioning properly.

▶ Procedure

To test the LEDs:

1. Position the cursor at the Start command next to Lamp Test on the Card Tests screen.
2. Press Enter.

   The Start command is changed to Stop. During the Lamp test, all LEDs blink simultaneously every second. When you stop the Lamp test, the LEDs are restored to their normal condition.
3. To stop the lamp test, position the cursor at the Stop command.
4. Press Enter.

Ending an Active Test

Except for the Remote Send Line Loopback and Remote DCLB, a test initiated by the user can be ended by the user. Tests can also be terminated automatically by enabling the Test Timeout option from the System Options Menu.

- A Test Timeout option is available to automatically terminate a user-initiated Loopback or Pattern test (as opposed to manually terminating a test) after it has been running a specified period of time. The default is 10 minutes. Refer to Table A-3, System Options.

  Test Timeout does not pertain to tests initiated by the network.

- On each test screen is a Command column. To stop the test, press Enter when the cursor is on the Stop command.

- Use the Abort All Tests selection from the Test menu to stop all tests running on all interfaces, with the exception of network-initiated loopbacks. **`Command Complete`** appears when all tests on all interfaces have been terminated.

  An aborted test may continue to run for a few seconds as the abort command is sent to the remote end and processed.

Messages and Troubleshooting

6

Overview

There are many resources available to assess the status of the device and contribute to problem resolutions. Refer to the following sections:

- *Configuring SNMP Traps*
- *Device Messages*
- *Troubleshooting*

Configuring SNMP Traps

An SNMP trap can be automatically sent out through the EOC or the Management port to an SNMP manager when the 7986 Standalone Termination Unit detects conditions set by the user. These traps enable the SNMP manager to gauge the state of the network. Refer to Appendix B, *Standards Compliance for SNMP Traps*, for details of SNMP traps supported by the 7986 Standalone Termination Unit.

To configure the 7986 Standalone Termination Unit for SNMP traps, use the SNMP Traps Options screen to:

- Enable SNMP traps.
- Set the number of SNMP managers that receive SNMP traps from the 7986 Standalone Termination Unit by entering an IP address and network destination for each SNMP manager specified.
- Select the type of SNMP traps to be sent from the 7986 Standalone Termination Unit.

To configure SNMP Traps, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Management and Communication Options → SNMP Traps Options

```
main/config/management/trap                                          Hotwire
                                                                   Model: 7986


                              SNMP TRAPS OPTIONS

     SNMP Traps:          Enable          Number of Trap Managers: 5

     NMS 1 IP Address:   135.014.040.001  Clear    Destination: DSL
     NMS 2 IP Address:   135.014.003.027  Clear    Destination: DSL
     NMS 3 IP Address:   135.014.001.008  Clear    Destination: DSL
     NMS 4 IP Address:   135.014.002.024  Clear    Destination: DSL
     NMS 5 IP Address:   204.128.146.035  Clear    Destination: DSL


     General Traps:              Both
     Enterprise Specific Traps: Enable
     Link Traps:                 Both
     Link Traps Interfaces:      Network


--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
 Save
```

Refer to Table A-7, SNMP Traps Options to configure SNMP traps.

Device Messages

The Device Messages in Table 6-1, listed in alphabetical order, can appear in the messages area at the bottom of the ATI screens.

Table 6-1. Device Messages (1 of 2)

Device Message	What Message Indicates	What To Do
Access level is Operator. Configuration is read-only.	The operator requested that configuration options be loaded, but does not have authority to edit them.	If configuration options are to be edited, use a Login ID that has Administrator authority.
Cannot Save – no Login IDs with Access Administrator	All of the login IDs being saved have an access level below Administrator.	Change the access level of at least one Login ID to Administrator so that configuration changes can be made. (Operator-level users cannot make configuration changes.) Save the Login IDs.
Command Complete	Action requested has successfully completed.	No action needed.
Invalid Character (*x*)	A nonprintable ASCII character (*x*) has been entered.	Reenter information using valid characters.
Invalid – Data Terminal Initiated Loopback Active	Network-initiated loopback was in progress when another selection was made.	No action needed.
Invalid Password	Login is required and an incorrect password was entered; access is denied.	■ Try again. ■ Contact your system administrator to verify your password.
Invalid – Send Pattern Already Active	A pattern test was already in progress when the Start field was selected.	■ Allow test to continue. ■ Select another test. ■ Stop the test.
Invalid – [Test] Already Active	The described test was already in progress when another selection was made.	■ Allow test to continue. ■ Select another test. ■ Stop the test.
Invalid Test Combination	A loopback or pattern test was in progress when Start was selected to start another test, or was active on the same or another interface when Start was selected.	■ Wait until other test ends and message clears. ■ Abort all tests from the Test menu screen. ■ Stop the test from the same screen the test was started from.

Table 6-1. Device Messages (2 of 2)

Device Message	What Message Indicates	What To Do
Invalid entry at cursor *(1...223, excluding 127)*	Invalid range.	Enter a value within the IP address range.
Limit of six Login IDs reached	An attempt to enter a new login ID was made, and the limit of six login/password combinations has been reached.	1. Delete another login/password combination. 2. Reenter the new login ID.
No Security Records to Delete	Delete was selected from the Administer Login screen, and no security records had been defined.	■ No action needed. ■ Enter a security record.
Password Matching Error – Re-enter Password	Password entered in the Reenter Password field of the Administer Logins screen does not match what was entered in the Password field.	■ Try again. ■ Contact your system administrator to verify your password.
Please Wait	Command takes longer than 5 seconds.	Wait until message clears.
Test Active	A test is running and no higher priority health and status messages exist.	■ Contact service provider if test initiated by the network. ■ Wait until the other test ends and message clears. ■ Cancel all tests from the Test screen. ■ Stop the test from the same screen the test was started from.
0.0.0.0 is an invalid IP address	An IP address of all zeroes was entered.	Enter a valid, non-zero IP address.

Troubleshooting

This 7986 Standalone Termination Unit is designed to provide you with many years of trouble-free service. If a problem occurs, however, refer to Table 6-2 for possible solutions.

Table 6-2. Troubleshooting (1 of 2)

Symptom	Possible Cause	Solutions
Alarm LED is on.	One of several alarm conditions exists. Health and Status displays the alarm condition.	Refer to Table 4-1, Health and Status Messages, for recommended action.
Cannot access the unit via the ATI.	The terminal is not set up for the correct rate or data format, or the unit is configured so it prevents access.	■ Check the cable and connections. ■ Ensure the unit is configured properly. Verify IP address and communication port usage. ■ Reset the unit.
Device Fail appears on the System and Test Status screen under Self-Test results.	The unit detects an internal hardware failure.	■ Reset the unit. ■ Contact your service representative.
No power, or the LEDs are not lit.	The power cord is not securely plugged into the wall receptacle and into the rear panel connection.	Check that the power cord is securely attached at both ends.
	The wall receptacle has no power.	■ Check the wall receptacle power by plugging in some equipment that is known to be working. ■ Check the circuit breaker. ■ Verify that your site is not on an energy management program.
	Power supply has failed.	Replace power supply.
An LED is not lit.	LED is out.	Run the Lamp test. If the LED in question does not flash with the other LEDs, then contact your service representative.

Table 6-2. Troubleshooting (2 of 2)

Symptom	Possible Cause	Solutions
Not receiving data.	■ The network or data port cables are not connected (check front panel LEDs for more information). ■ No crossover cable being used on the DSL network. ■ A test is being executed on the unit (check the TEST LED on the front panel). ■ The far-end device is off-line.	■ Check network and data port cables. ■ Run Loopback tests. Refer to Chapter 5, *Testing*. ■ Use a crossover cable on the DSL network. Cross Pins 1, 2 to 4, 5. ■ Stop the test or wait for the test to end. ■ Make sure the far-end device is on.
Power-Up Self-Test fails. Only Alarm LED is on after power-up.	The unit has detected an internal hardware failure.	■ Reset the unit and try again. ■ Contact your service representative.

Security

7

Overview

The 7986 Standalone Termination Unit provides several methods of security by limiting user access to the ATI through option settings. You can:

- Enable the Telnet Login Required option.
- Limit the access by setting a Session Access Level option of Operator for the Telnet Session.
- Disable the access with the Telnet Session option.

See Table A-5, Telnet Sessions Options, in Appendix A, *Configuration Option Tables*.

ATI Access Levels

The 7986 Standalone Termination Unit has two access levels: Administrator and Operator. The access level determines what functions are accessible, as shown in Table 7-1.

Table 7-1. Access Levels

ATI Access to Menu Functions	Administrator	Operator
Status	Read-Only	Read-Only
Test	Full Access	No Access
Configuration	Full Access	Read-Only
Control	Full Access	No Access

The effective access level is the more restrictive of the session access level or the login access level.

Access level is also used to control access via Telnet. If the Telnet Session Access Level is set to Administrator (see Table A-5, Telnet Session Options), a Login ID with an Operator access level is not permitted access.

Creating a Login

Logins apply to the terminal directory connected to the communication port or Telnet access directly to the ATI of the 7986 Standalone Termination Unit.

Six login ID/password combinations are available. Each Login ID and Password must be unique and include an access level.

▶ Procedure

1. To create a login record, follow this menu selection sequence:

   Main Menu → Control → Administer Logins

```
main/control/admin_logins                                          Hotwire
                                                                 Model: 7986


                              ADMINISTER LOGINS                  Page 1 of x

                         Login ID:           newuser
                         Access Level:       Administrator



                              Are you sure? Yes

--------------------------------------------------------------------------------
                                    ESC for previous menu       MainMenu   Exit
 Save   PgUp   PgDn                                             New        Delete
```

2. Select Newuser and press Enter. The Login Entry screen appears.

```
main/control/admin_logins                                          Hotwire
Slot: 4                                                          Model: 7986


                                    LOGIN ENTRY

                               Login ID:           newuser2___
                               Password:           es342_____
                               Re-enter Password:  es342_____
                               Access Level:       Administrator

                                    WARNING
                      New logins will not become permanent until saved
                          through the "ADMINISTER LOGINS" screen!

--------------------------------------------------------------------------------
Ctrl-a to access these functions  ESC for previous menu       MainMenu   Exit
 Save
```

3. Create the login by entering the following fields. Login IDs and passwords are case-sensitive.

On the Login Entry screen, for the . . .	**Enter . . .**
Login ID	1 to 10 ASCII printable characters (hex21 through 7E). Blanks are not allowed.
Password	1 to 10 ASCII printable characters that can consist of 0–9, a–z, A–Z, # (pound), . (period), – (dash), and / (slash).
Re-enter Password	1 to 10 ASCII printable characters characters that can consist of 0–9, a–z, A–Z, # (pound), . (period), – (dash), and / (slash).
Access Level	Administrator, Operator

NOTE:

Assign at least one Administrator-level Login ID. Full access is necessary to make configuration option changes and administer logins.

4. Press Ctrl-a to switch to the screen function key area below the dotted line. Select Save and press Enter.
5. When Save is complete, **`Command Complete`** appears at the bottom of the screen.
6. If additional logins are required, repeat Steps 3 through 5.
7. When all logins are entered, press Esc to return to the Administer Logins screen.
8. Select Save and press Enter.

Deleting a Login

▶ Procedure

1. To delete a login record, follow this menu selection sequence:

   Main Menu → Control → Administer Logins

2. Select PgUp or PgDn and press Enter to page through login pages/records until you find the one to be deleted.

3. Once the correct record is displayed, select Delete and press Enter.

4. To complete the delete action, select Save and press Enter.

   When the deletion is complete, **`Command Complete`** appears at the bottom of the screen. The number of login pages/records reflects one less record, and the record following the deleted record appears.

Controlling SNMP Access

There are three methods for limiting SNMP access.

- Disable the SNMP management option. Refer to Table A-8, General SNMP Management Options.
- Assign SNMP community names and access types.
- Limit SNMP access through validation of the IP address of each allowed SNMP manager.

Assigning SNMP Community Names and Access Types

The unit can be managed by an SNMP manager supporting SNMP. The community name must be supplied by an external SNMP manager accessing an object in the MIB.

To define SNMP community names, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → SNMP → General SNMP Management

Refer to Table A-8, General SNMP Management Options, to:

- Enable SNMP Management.
- Assign the SNMP community names of the SNMP Managers that are allowed to access the unit's Management Information Base (MIB).
- Specify Read or Read/Write access for each SNMP community name.

Limiting SNMP Access through the IP Addresses of the Managers

The unit provides an additional level of security through validation of the IP addresses.

The SNMP Management option must be enabled. To control SNMP access with IP addresses, follow this menu selection sequence:

Main Menu → *Configuration* → *Management* → *Security Menu*

Refer to Table A-9, SNMP NMS Security Options. The SNMP access can be limited by:

- Enabling NMS IP address checking.
- Add each IP address and access level.

NOTE:

Do not change or delete the IP address or access level of the NMS performing the sets or enable IP address checking prior to adding the NMS to the table.

Resetting the Termination Unit's COM Port or Factory Defaults

Misconfiguring the termination unit could render the user interface inaccessible, leaving it in a state where a session cannot be started via the COM port or a Telnet session. If this occurs, the termination unit connectivity can be restored via a terminal directly connected to the COM port.

Two methods can be used to restore access to the user interface:

- **Reset COM Port** – Allows you to reset the configuration options related to COM port usage. This also causes a device reset, where the termination unit performs a Device Self-Test. No security-related configuration options are changed.
- **Reload Factory Defaults** – Allows you to reload the Default Factory Configuration, resetting all of the configuration and control settings which causes the current configuration to be destroyed and a device reset. This method is also useful when the user's password(s) have been forgotten.

▶ Procedure

To reset COM port settings:

1. At the terminal that is directly connected to the unit's COM port, configure the terminal to operate at 9.6 kbps, using character length of 8 bits, with one stop-bit, and no parity.
2. Reset the unit, then immediately and repeatedly press Enter at a rate of about 1 press per second until the System Paused screen appears.
3. Tab to the desired method, and enter **yes** (or **y**) for the selected prompt.

If entering yes to prompt . . .	Then . . .
Reset COM Port usage	■ Port type is set to Terminal ■ Data Rate (kbps) is set to 9.6 ■ Character Length is set to 8 ■ Stop Bits is set to 1 ■ Parity is set to None
Reload Factory Defaults	Yes (or y) will restore all factory-loaded configuration and control settings contained in the Default Factory Configuration area are loaded.

If no (or n) is entered, or if no selection is made within 30 seconds, the unit returns to the condition or operation it was in when the system reset was initiated, with the COM port rate returning to its configured rate.

The termination unit resets itself, going through a Self-Test. Connectivity is restored and the Main Menu screen appears.

IP Addressing

8

Selecting an IP Addressing Scheme

The NTU's network interface IP address is assigned through the peer IP address of the LTU's Network Interface menu. The NTU obtains the LTU's IP address and subnet mask when the PPP link is established over the EOC. The LTU IP address and subnet mask are configured from the Communication Protocol Options menu.

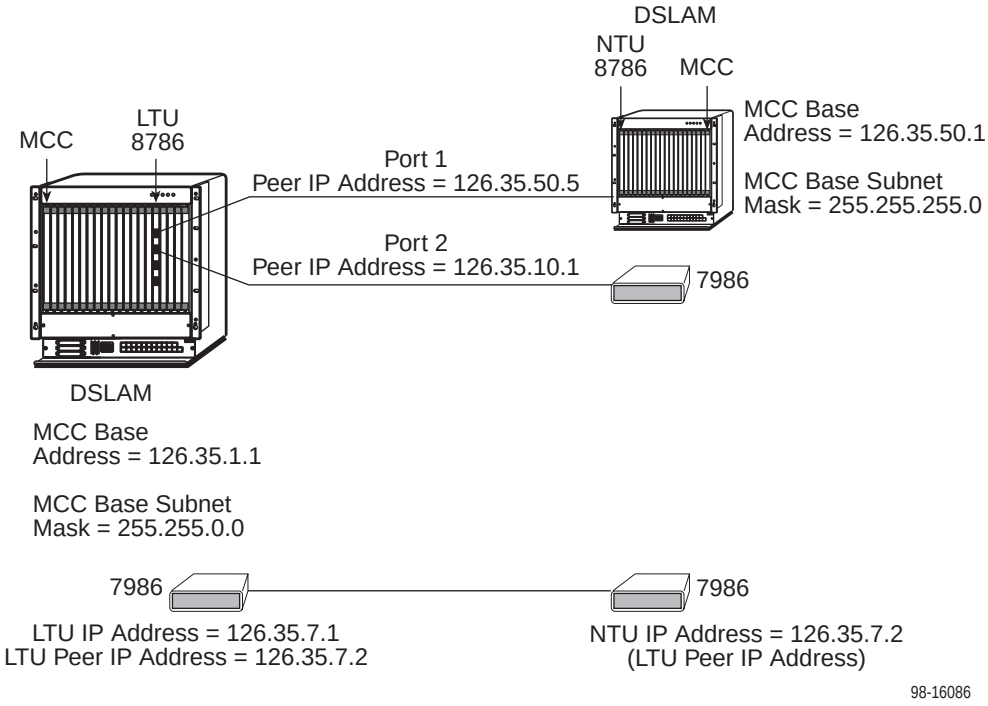
The 7986 Standalone Termination Unit is assigned an IP address and subnet through the Peer IP address of the MHDSL Network interface menu. Once the address is assigned, you can use the 7986 Standalone Termination Unit's ATI to assign:

- An IP address for each NMS. For SNMP IP configuration options, see Table A-7, SNMP Traps Options, Table A-8, General SNMP Management Options, and Table A-9, SNMP NMS Security Options, in Appendix A, *Configuration Option Tables*.
- An IP address for the TFTP server you wish to use to upload and download configurations. See *Configuration Loader* in Chapter 3, *Initial Setup and Configuration*.

Review the following information in preparation for selecting an IP addressing scheme.

- Any legal host address is allowed for a given subnet. The address choice within the subnet is arbitrary.
- A single route to a subnet is all that is needed to reach every device on a subnet.

IP Addressing Example



Peer IP Address Assignments

- The Peer IP Address refers to the IP address of the unit configured as an NTU.
- The Peer IP Address is assigned by the LTU.

Configuration Option Tables

A

Overview

The tables in this appendix summarize the configuration options accessed when you select the Configuration option on the Main Menu. The Configuration options are arranged into groups based upon functionality.

Select . . .	To Access the . . .	To Configure the . . .
Network	Network Interface Options, Table A-1	E1 HDSL network interface Ports.
G.703 Interface	G.703 Interface Options, Table A-2	G.703 interface port.
System	System Options, Table A-3	General system options of the unit.
Communication Port	Communication Port Options, Table A-4	Unit's COM port options.
Management and Communication	■ Telnet Session Options, Table A-5 ■ Communication Protocol Options, Table A-6 ■ SNMP Traps Options, Table A-7 ■ General SNMP Management Options, Table A-8 ■ SNMP NMS Security Options, Table A-9	Management support of the unit through SNMP and Telnet.

NOTE:

All changes to configuration options must be saved. Refer to *Saving Configuration Options* in Chapter 3, *Initial Startup and Configuration*.

Network Interface Options Menu

For Network Interface Options, refer to Table A-1. To access the Network Interface Options screen, follow this menu selection sequence:

Main Menu → Configuration → Current Configuration → Network

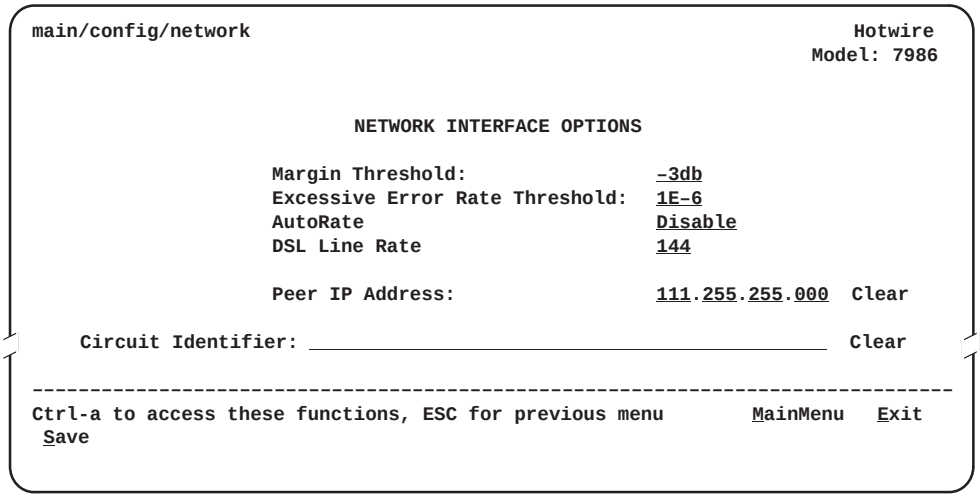


Table A-1. Network Interface Options (1 of 2)

Margin Threshold
Possible Settings: **–5db**, **–4db**, **–3db**, **–2db**, **–1db**, **0db**, **1db**, **2db**, **3db**, **4db**, **5db**, **6db**, **7db**, **8db**, **9db**, **10db** Default Setting: **0db**
Determines the level, expressed in decibels, at which a signal-to-noise margin condition is recognized. **–5db** to **10db** – Sets the margin threshold to this value.
Excessive Error Rate Threshold
Possible Settings: **1E–4**, **1E–5**, **1E–6**, **1E–7**, **1E–8**, **1E–9** Default Setting: **1E–6**
Determines the error rate at which an excessive error rate (EER) condition is recognized. The rate is the ratio of the number of CRC errors to the number of bits received in a certain period.
AutoRate (LTU only)
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether the DSL line will automatically train up to the best rate or be user selectable. This option is only available when the standalone unit is configured as an LTU. **Enable** – The LTU is set to automatically adjust at the best line rate. **Disable** – The LTU Line rate is user selectable and is based on the DSL Line Rate selected.

Table A-1. Network Interface Options (2 of 2)

DSL Line Rate
Possible Settings: **144, 272, 400, 528, 784, 1040, 1552, 2064** Default Setting: **2064**
Specifies the DSL line rate of the unit. This option is only available when the standalone unit is configured as an LTU and AutoRate is disabled (unit is in fixed rate). **400** – The DSL Line rate is 400. **528** – The DSL Line rate is 528. **784** – The DSL Line rate is 784. **1040** – The DSL Line rate is 1040. **1552** – The DSL Line rate is 1552. **2064** – The DSL Line rate is 2064. NOTE: For associated payload rates refer to Table 3-4, Fixed Rate Payload Rates and DSL Line Rates in Chapter 3, *Initial Startup and Configuration*.
Peer IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the peer IP address for the remote management providing the remote management link on the DSL loop. This option is only available when the standalone unit is configured as an LTU. The Peer IP Address is must be in the same subnet **Address Field** – **(000.000.000.001 – 223.255.255.255)** – Enter an address for the peer unit. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. The peer IP address must be in the same subnet as the MCC address. **Clear** – Clears the IP address field and sets to all zeros.
Circuit Identifier
Possible Settings: **[ASCII Text], Clear** Default Setting: [blank]
Uniquely identifies the circuit number of the transmission vendor's DSL line for troubleshooting purposes. **[ASCII Text]** – Enter a maximum of 128 characters. All printable ASCII characters except ^ (caret) are allowed. **Clear** – Clears the field.

G.703 Interface Options Menu

For G.703 Interface Options, refer to Table A-2. To access the G.703 Interface Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → G.703

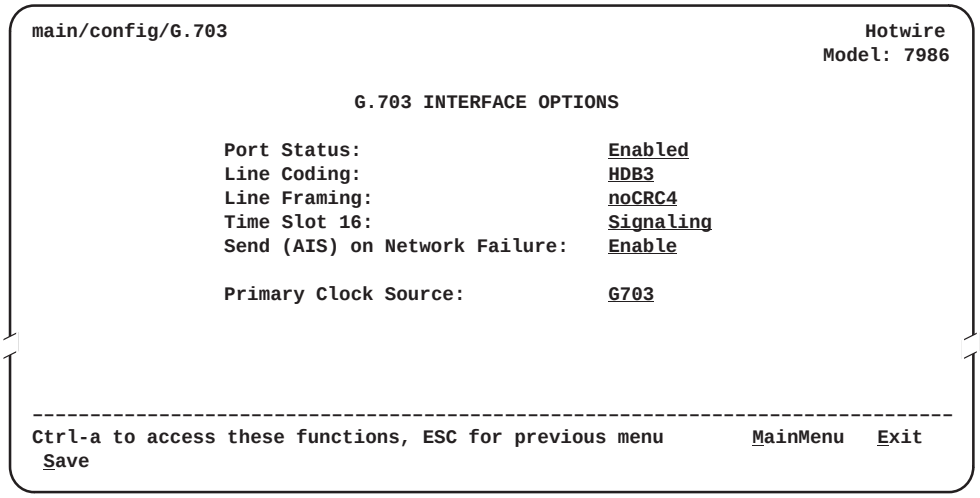


Table A-2. G.703 Interface Options (1 of 2)

Port Status
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines if the port can be configured and used to receive and transmit data. **Enable** – The port can be configured to transmit and receive data. **Disable** – The port can not be configured and does not receive or transmit data. No alarms or traps associated with the port will be generated. The LED associated with the port is held in the OFF state
Line Coding Format
Possible Settings: **AMI, HDB3** Default Setting: **HDB3**
Specifies the line coding format to be used by the G.703 interface. **AMI** – Indicates the line coding format used by the G.703 interface is Alternate Mark Inversion (AMI). **HDB3** – Indicates the line coding format used by the G.703 interface is HDB3.

Table A-2. G.703 Interface Options (2 of 2)

Line Framing
Possible Settings: **CRC4, noCRC4** Default Setting: **noCRC4**
Specifies the framing format to be used by the G.703 interface. **CRC4** – CRC4 framing formatting is used for transmitted and received data over the Network Interface. **noCRC4** – Non-CRC4 framing format is used for transmitted and received data over the Network Interface.
Time Slot 16
Possible Settings: **Signaling, Data** Default Setting: **Signaling**
Specifies weather the G.703 interface is used for voice or data. **Signaling** – Timeslot 16 is used for signalling (the unit is in voice mode). **Data** – Timeslot 16 is used for data (the unit is in data mode). NOTE: For associated DSL line rates and payload rates refer to Table 3-4, Fixed Rate Payload Rates and DSL Line Rates in Chapter 3, *Initial Startup and Configuration*.
Primary Clock Source
Possible Settings: **G.703, Internal** Default Setting: **Internal**
Specifies where the unit will derive its timing from. **Internal** – The clock source is derived from the internal oscillator. **G.703 Pt1** – The clock source is derived from the G.703 interface.
Possible Settings: **1E–4**, **1E–5**, **1E–6**, **1E–7**, **1E–8**, **1E–9** Default Setting: **1E–4**
Determines the error rate at which an excessive error rate (EER) condition is recognized. The rate is the ratio of the number of CRC errors to the number of bits received in a certain period.
Send AIS on Network Failure
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies the action taken on the signal transmitted to the G.703 when a valid signal cannot be recovered from the network interface (LOS or cognitions OOF, AIS, or EER). **Enable** – An Alarm Indication Signal (AIS) is sent to the DTE in the event an LOS or continuous OOF, AIS, or EER condition exists on the G.703 interface. **Disable** – The failed signal on the interface is sent to the DTE in the event an LOS or continuous OOF, AIS, or EER condition exists on the G.703 interface.

System Options Menu

For System Options, refer to Table A-3. To access the System Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → System

```
main/config/system                                                    Hotwire
                                                                  Model: 7986


                              SYSTEM OPTIONS

                    DSL Mode:                    NTU
                    Test Timeout:                Enable
                    Test Duration (min):         10

                    G.703 Line Termination       120 Ohm


--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu        MainMenu   Exit
 Save
```

Table A-3. System Options

DSL Mode
Possible Settings: **LTU**, **NTU** Default Setting: **NTU**
Controls whether the unit is configured as a control unit or tributary unit. **LTU** – The unit is configured as a control unit (Line Termination Unit). **NTU** – The unit is configured as a tributary unit (Network Termination Unit). This unit will request its IP address from the LTU during establishment of the PPP link. NOTE: Changing this option will reset the card.
Test Timeout
Possible Settings: **Enable**, **Disable** Default Setting: **Enable**
Allows user-initiated tests to end automatically. The feature should be enabled when the unit is remotely managed, so that control can be regained after a test is accidentally executed. **Enable** – User-initiated loopback and pattern tests end when test duration is reached. **Disable** – Tests can be terminated manually from the Network Tests screen. Refer to *Running Network Tests* in Chapter 5, *Testing*. NOTE: Tests commanded by the DTE or network-initiated tests are not affected by this test timeout.

Table A-3. System Options

Test Duration (min)
Possible Settings: **1–120** Default Setting: **10**
Number of minutes for a test to be active before automatically ending. ■ The Test Duration (min) option appears when Test Timeout is enabled. **1** to **120** – Amount of time in minutes for a user-initiated test to run before terminating.
G.703 Line Termination
Possible Settings: **75 ohms, 120 ohms** Default Setting: **120 ohms**
Specifies the impedance of the G.703 interface **75 ohms** – The G.703 interface impedance is 75 ohms unbalanced. **120 ohms** – The G.703 interface impedance is 120 ohms balanced.

Communication Port

For Communication Port Options, refer to Table A-4. To access the Communications Ports screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Communication Port

```
main/config/commport                                              Hotwire
                                                                Model: 7986


                          COMMUNICATION PORT OPTIONS

                    Port Use:                   Terminal
                    Port Type:                  Asynchronous
                    Data Rate (Kbps):           9.6
                    Character Length:           8
                    Parity:                     None
                    Stop Bits:                  1
                    Ignore Control Leads:       Enable

                    Login Required:             Enable
                    Port Access Level:          Administrator
                    Inactivity Timeout:         Enable
                    Disconnect Time (Minutes):  5


--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
```

Table A-4. Communication Port Options (1 of 3)

Port Use
Possible Settings: **Terminal**, **Net Link** Default Setting: **Terminal**
Specifies how the communications port is to be used. **Terminal** – The communication port will be used for the Asynchronous terminal interface. **Net Link** – The communication port will be used as the network communication link to an IP network or device.
Port Type
Possible Settings: **Asynchronous**, **Synchronous** Default Setting: **Asynchronous**
When Port Use is set to Net Link, Port Type controls whether the communication port will be asynchronous or synchronous. **Asynchronous** – Configures the communication port for asynchronous communication. **Synchronous** – Configures the communication port for synchronous communication. NOTE: Peer IP Address and Circuit Identifier are *not* copied.

Table A-4. Communication Port Options (2 of 3)

Data Rate
Possible Settings: **9.6**, **14.4, 19.2, 28.8, 38.4** Default Setting: **9.6**
Specifies the communication port baud rate. **9.6** – Communication port rate is 9600 bps (Terminal). **14.4** – Communication port rate is 14400 bps (Netlink). **19.2** – Communication port rate is 19200 bps (Netlink). **28.8** – Communication port rate is 28800 bps (Netlink). **38.4** – Communication port rate is 38400 bps (Netlink).
Character Length (Asynchronous mode only)
Possible Settings: **7, 8** Default Setting: **8**
Determines the character length of the communication port. **7** – The character length of the communication port is seven bits. **8** – The character length of the communication port is eight bits.
Parity (Asynchronous mode only)
Possible Settings: **None**, **Odd, Even** Default Setting: **None**
Specifies the parity of the communication port. **None** – No parity used. **Odd** – Odd parity used. **Even** – Even parity used.
Stop Bits (Asynchronous mode only)
Possible Settings: **1, 1.5, 2** Default Setting: **1**
Specifies the number of stop bits for the communication port. **1** – One stop bit. **1.5** – One and one half stop bits**.** **2** – Two stop bits used**.**
Ignore Control Leads (Asynchronous mode only)
Possible Settings: **Disable, DTR** Default Setting: **Disable**
Specifies whether DTR is used. **Disable** – Control leads are treated as standard. **DTR** – DTR is ignored**.**

Table A-4. Communication Port Options (3 of 3)

Login Required (Asynchronous mode only)
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies if an ID and password are required to access the asynchronous terminal interface on the communication port. Login IDs are created with a password and access level. Refer to Chapter 7, *Creating a Login*. **Enable** – Login ID and password are required to access the asynchronous terminal interface. **Disable** – No Login ID and password are required to access the asynchronous terminal interface.
Port Access Level (Asynchronous mode only)
Possible Settings: **Administrator**, **Operator** Default Setting: **Administrator**
Specifies the highest level of access allowed when accessing an ATI session through a Telnet session. **Administrator** – This is the higher access level, permitting full control of the 7986 Termination Unit. Access level is determined by the Login ID. If Telnet Login Required is disabled, the session access level is Administrator. **Operator** – This is the lower access level, permitting read-only access to status and configuration screens.
Inactivity Timeout (Asynchronous mode only)
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Provides automatic logoff of a Telnet session. **Enable** – The Telnet session terminates automatically after the Disconnect Time. **Disable** – A Telnet session will not be closed due to inactivity.
Disconnect Time (Minutes) (Asynchronous mode only)
Possible Settings: **1 – 60** Default Setting: **5**
Number of minutes of inactivity before the session terminates automatically. Timeout is based on no keyboard activity. ■ Disconnect Time (minutes) option appears when Inactivity Timeout is enabled. **1** to **60** – The Telnet session is closed after the selected number of minutes.

Management and Communication Options Menu

The Management and Communication Options Menu includes the following:

- Telnet Session Options, Table A-5
- Communication Protocol Options, Table A-6
- SNMP Traps Options, Table A-7
- General SNMP Management Options, Table A-8
- SNMP NMS Security Options, Table A-9

Telnet Session Options

The Telnet session configuration options control whether a Telnet session is allowed through an interconnected IP Network. If allowed, these options determine what level of security to apply to the session to control access. Only one Telnet session is allowed at a time. Initial values are determined by the configuration you currently have loaded. To access the Telnet Session Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Management and Communication → Telnet Session

```
main/config/telnet                                                Hotwire
                                                                Model: 7986


                          TELNET SESSION OPTIONS

                    Telnet Session:                 Enable
                    Telnet Login Required:          Enable
                    Session Access Level:           Administrator
                    Inactivity Timeout:             Enable
                    Disconnect Time (Minutes)       5




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
 Save
```

Table A-5. Telnet Session Options

Telnet Session
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies if the Termination Unit will respond to a Telnet session request from a Telnet client on an interconnected IP network. **Enable** – Allows Telnet sessions between the unit and a Telnet client. **Disable** – No Telnet sessions allowed.
Telnet Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether a user ID and password are required to access to the ATI through a Telnet session. Login IDs are created with a password and access level. Refer to *Creating a Login* in Chapter 7, *Security*. **Enable** – Security is enabled. When access is attempted via Telnet, the user is prompted for a Login ID and password. **Disable** – No Login required for a Telnet session.
Session Access Level
Possible Settings: **Administrator**, **Operator** Default Setting: **Administrator**
The Telnet session access level is interrelated with the access level of the Login ID. Refer to *ATI Access Levels* in Chapter 7, *Security* for more information. **Administrator** – This is the higher access level, permitting full control of the 7986 Termination Unit. Access level is determined by the Login ID. If Telnet Login Required is disabled, the session access level is Administrator. **Operator** – This is the lower access level, permitting read-only access to status and configuration screens.
Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Provides automatic logoff of a Telnet session. **Enable** – The Telnet session terminates automatically after the Disconnect Time. Set the Disconnect time (in minutes) after enabling Inactivity Timeout **Disable** – A Telnet session will not be closed due to inactivity.
Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **5**
Number of minutes of user inactivity before a Telnet session terminates automatically. Time out is based on no keyboard activity. ■ Disconnect Time (minutes) option appears only when the Inactivity Timeout option is enabled. **1** to **60** – The Telnet session is closed after the selected number of minutes.

Communication Protocol Options

The communication protocol configuration options specify the information necessary to support the IP communication network, including; IP address and link protocols. Initial values are determined by the configuration you currently have loaded. To access the Communication Protocol Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Management and Communication → Comm Protocol Options

```
main/config/management/communication                              Hotwire
                                                                Model: 7986


                        COMMUNICATION PROTOCOL OPTIONS

                Node IP Address:                 000.000.000.000    Clear
                Node Subnet Mask:                000.000.000.000    Clear

                Default Network Destination:     None

                Communication Port
                  IP Address:                    000.000.000.000    Clear
                  Subnet Mask:                   000.000.000.000    Clear
                  Link Protocol:                 PPP




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu        MainMenu   Exit
```

Table A-6. Communication Protocol Options (1 of 2)

Node IP Address
Possible Settings: **000.000.000.000** – **223.255.255.255** Default Setting: **000.000.000.000**
Specifies the Node IP address. This option is only available when the standalone unit is configured as an LTU. **Address Field** – **(000.000.000.000** – **223.255.255.255)** – Enter an IP address for the node. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. **Clear** – Clears the IP address field and sets to all zeros.
Node Subnet Mask
Possible Settings: **000.000.000.000** – **255.255.255.255** Default Setting: **000.000.000.000**
Specifies the Node Subnet Mask. This option is only available when the standalone unit is configured as an LTU. **Address Field** – **(000.000.000.000** – **255.255.255.255)** – Enter an address for the Node Subnet Mask. **Clear** – Clears the address field and sets to all zeros.
Default Network Destination
Possible Settings: **None**, **COM, DSL** Default Setting: **None**
Specifies where the default management network is connected, for example, if your default network is connected to the COM port, select COM as the default management network destination. **None** – No default destination is defined. Data that cannot be routed is discarded. **COM** – The unit's COM port is the default network destination. This option is only available when the Port Use option on the Communication Port Options menu is set to Net Link. **DSL** – The unit's DSL port is the default network destination.
Communication Port IP Address
Possible Settings: **000.000.000.000** – **223.255.255.255** Default Setting: **000.000.000.000**
Specifies the unit's Communication Port IP Address when the unit is configured as a network communication link. This option is only used when the Port Use option on the Communication Port Options menu is set to Net Link. If the COM Port IP address is not set (000.000.000.000) the node IP address specified by the Node IP Port will be used. **Address Field** – **(000.000.000.000** – **223.255.255.255)** – Enter an IP address for the Communication Port. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. **Clear** – Clears the IP address and sets to all zeros.

Table A-6. Communication Protocol Options (2 of 2)

Communication Port Subnet Mask
Possible Settings: **000.000.000.000** – **255.255.255.255** Default Setting: **000.000.000.000**
Specifies the unit's Communication Port Subnet Mask when the unit is configured as a network communication link. This option is only used when the Port Use option on the Communication Port Options menu is set to Net Link. If the COM Port IP address is not set (000.000.000.000), the node IP Address will be used. **Address Field** – **(000.000.000.000** – **255.255.255.255)** – Enter an address for the Communication Port Subnet Mask. **Clear** – Clears the address and sets to all zeros.
Communication Port Link Protocol
Possible Settings: **PPP**, **SLIP** Default Setting: **PPP**
Specifies the unit's Communication Port link layer protocol when the unit is configured as a network communication link. This option is only used when the Port Use option on the Communication Port Options menu is set to Net Link. **PPP** – Defines Point-to-Point protocol for the link layer protocol for the network communication link. **SLIP** – Serial Line IP Protocol for the link layer protocol for the network communication link.

SNMP Traps Options

SNMP configuration options allow you to specify the information necessary to support the 7986 Termination unit SNMP traps. To access the SNMP Traps Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → Management and Communication → SNMP Traps

```
main/config/management/trap                                        Hotwire
                                                                 Model: 7986


                              SNMP TRAPS OPTIONS

     SNMP Traps:          Enable           Number of Trap Managers: 5

     NMS 1 IP Address:   135.014.040.001  Clear    Destination: IMC
     NMS 2 IP Address:   135.014.003.027  Clear    Destination: IMC
     NMS 3 IP Address:   135.014.001.008  Clear    Destination: IMC
     NMS 4 IP Address:   135.014.002.024  Clear    Destination: IMC
     NMS 5 IP Address:   204.128.146.035  Clear    Destination: IMC


     General Traps:              Both
     Enterprise Specific Traps:  Enable
     Link Traps:                 Both
     Link Traps Interfaces:      Network


--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu        MainMenu   Exit
 Save
```

Table A-7. SNMP Traps Options (1 of 2)

SNMP Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls the generation of SNMP trap messages. The options for addresses and types of traps are located in this table. **Enable** – SNMP trap messages are sent out to SNMP managers. **Disable** – No SNMP trap messages are sent out.
Number of Trap Managers
Possible Settings: **1, 2, 3, 4, 5** Default Setting: **1**
Sets the number of SNMP management systems that will receive SNMP traps. **1 to 5** – Number of trap managers. An NMS IP address is required for each manager.
NMS *n* IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the Internet Protocol address used to identify each SNMP trap manager. **Address Field** – **(000.000.000.000 – 223.255.255.255)** – Enter an address for each SNMP trap manager. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. **Clear** – Clears the IP address and sets to all zeros.
NMS *n* Destination
Possible Settings: **DSL, COM** Default Setting: **DSL**
Provides the network destination path of each trap manager. **DSL** – The DSL port is the network destination path. **COM** – The COM port is the network destination path.
General Traps
Possible Settings: **Disable, Warm, AuthFail, Both** Default Setting: **Both**
Determines which SNMP traps are sent to each trap manager. **Disable** – No general trap messages are sent. **Warm** – Sends trap message for *warmStart* events. **AuthFail** – Sends trap message for *authenticationFailure* events. **Both** – Sends both trap messages. NOTE: Refer to Appendix B, *Standards Compliance for SNMP Traps*.

Table A-7. SNMP Traps Options (2 of 2)

Enterprise Specific Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines if SNMP traps are generated for enterprise-specific events. **Enable** – SNMP traps are generated for *enterpriseSpecific* events. NOTE: Refer to *Enterprise Specific Traps* in Appendix B, *Standards Compliance for SNMP Traps*. **Disable** – No enterprise-specific event traps are sent.
Link Traps
Possible Settings: **Disable, Up, Down, Both** Default Setting: **Both**
Determines if SNMP traps are generated for link up and link down for one of the communication interfaces. **Disable** – No *linkUp* or *linkDown* SNMP traps are generated. **Up** – A *linkUp* trap is generated when the 7986 Termination Unit recognizes that one of the communication interfaces is operational. **Down** – A *linkDown* trap is generated when the 7986 Termination Unit recognizes a failure in one of the communication interfaces. **Both** – Sends trap messages for detection of both *linkUp* and *linkDown*. NOTE: Refer to *linkUp and linkDown* in Appendix B, *Standards Compliance for SNMP Traps*.
Link Trap Interfaces
Possible Settings: **Network, SYNC, All** Default Setting: **All**
Determines if the SNMP *linkUp*, SNMP *linkDown*, and interface-related *enterpriseSpecific* traps are generated for the network interface, synchronous data (DTE) port, or both. **Network** – SNMP trap messages are generated for the network interface. **SYNC** – SNMP trap messages are generated for the synchronous data (DTE) port. **All** – SNMP trap messages are generated for the network E1 interface and the synchronous data (DTE) ports.

General SNMP Management Options

SNMP configuration options allow you to specify the information necessary to support the Termination Unit General SNMP functionality. To access the General SNMP Management Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → Management and Communication → SNMP → General SNMP Management

```
main/config/management/SNMP                                    Hotwire
Slot: 4                                                      Model: 8774


                        GENERAL SNMP MANAGEMENT OPTIONS

    SNMP Management:     Enable

    Community Name 1:    Public____
    Name 1 Access:       Read/Write
    Community Name 2:    Public____
    Name 2 Access:       Read/Write









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
 Save
```

Table A-8. General SNMP Management Options (1 of 2)

SNMP Management
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Enables or disables the SNMP management features. **Enable** – Enables SNMP management capabilities. **Disable** – Disables SNMP management capabilities.
Community Name 1
Possible Settings: **ASCII text field, Public** Default Text: **Public**
Identifies the name of the community allowed to access the unit's MIB. The community name must be supplied by an external SNMP manager when that manager attempts to access an object in the MIB. **Text Field** – Enter or edit a community name. **Clear** – Clears the community name field.

Table A-8. General SNMP Management Options (2 of 2)

Name 1 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Determines the access level for Community Name 1. **Read** – Allows read-only access (get) for Community Name 1. **Read/Write** – Allows read/write access (get) for Community Name 1.
Community Name 2
Possible Settings: **ASCII text field, Public** Default Text: **Public**
Identifies the name of the second community allowed to access the unit's MIB. The community name must be supplied by an external SNMP manager when that manager attempts to access an object in the MIB. **Text Field** – Enter or edit a community name. **Clear** – Clears the community name field.
Name 2 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Determines the access level for Community Name 2. **Read** – Allows read-only access (get) for Community Name 2. **Read/Write** – Allows read/write access (get/set) for Community Name 2.

SNMP NMS Security Options

SNMP configuration options allow you to specify the information necessary to support the Termination Unit SNMP NMS Security. To access the SNMP NMS Security Options screen, follow this menu selection sequence:

Main Menu → Configuration → Load Configuration From → Edit → Management and Communication → SNMP → Security

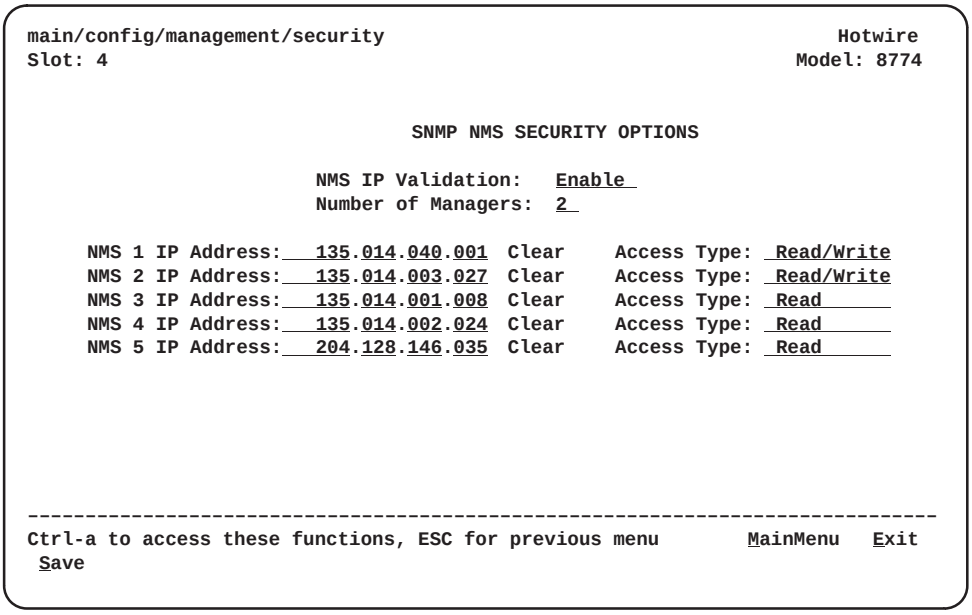

main/config/management/security
Hotwire
Slot: 4
Model: 8774
SNMP NMS SECURITY OPTIONS
NMS IP Validation: Enable
Number of Managers: 2
NMS 1 IP Address: 135.014.040.001 Clear Access Type: Read/Write
NMS 2 IP Address: 135.014.003.027 Clear Access Type: Read/Write
NMS 3 IP Address: 135.014.001.008 Clear Access Type: Read
NMS 4 IP Address: 135.014.002.024 Clear Access Type: Read
NMS 5 IP Address: 204.128.146.035 Clear Access Type: Read
Ctrl-a to access these functions, ESC for previous menu
MainMenu
Exit
Save

Table A-9. SNMP NMS Security Options (1 of 2)

NMS IP Validation
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether security checking is performed on the IP address of SNMP management systems attempting to access the node. **Enable** – Security checking is performed on the IP address of SNMP management systems attempting to access the node. **Disable** – No security checking is performed.
Number of Managers
Possible Settings: **1, 2, 3, 4, 5** Default Setting: **1**
Specifies the number of SNMP management systems that can send SNMP messages. **1 to 5** – Number of trap managers. An NMS IP address is required for each manager.

Table A-9. SNMP NMS Security Options (2 of 2)

NMS *n* IP Address
Possible Settings: **000.000.000.000 – 223.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the Internet Protocol address used to identify each SNMP manager. **000.000.000.000 – 223.255.255.255** – Enter an address for each SNMP manager. The range for the first byte is 000 to 223, with the exception of 127. The range for the remaining three bytes is 000 to 255. **Clear** – Clears the IP address and sets to all zeros.
Access Level
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Determines the access level allowed for an authorized NMS when IP address validation is being performed. **Read** – Allows read-only access (get) to the accessible objects in the MIB for this device. **Read/Write** – Allows read/write access (get/set) to the accessible objects in the MIB for this device.

Standards Compliance for SNMP Traps

B

SNMP Traps

This section describes the unit's compliance with SNMP standards and any special operational features for the SNMP traps supported. The unit supports the following traps:

- warmStart
- authenticationFailure
- linkUp
- linkDown

warmStart

SNMP Trap	Description	Possible Cause
warmStart	The unit has reinitialized itself. The trap is sent after the unit resets and stabilizes. There are no variable-bindings.	■ Reset command. ■ Power disruption.

authenticationFailure

SNMP Trap	Description	Possible Cause
authenticationFailure	Failed attempts to access the unit. There are no variable-bindings.	Three unsuccessful attempts were made to enter a correct login/password combination.

linkUp and linkDown

The link SNMP traps are:

- **linkUp** – The unit recognizes that one of the communication interfaces is operational.
- **linkDown** – The unit recognizes that one of the communication interfaces is not operational.

The network and synchronous port interfaces (physical sublayer) are represented by an entry in the MIB-II interfaces table and supported by the DS1 MIB.

The following list describes the conditions that define linkUp and linkDown:

linkUp/Down Variable-Bindings

- ifIndex (RFC 1573)

  This object provides the index into the ifTable and potentially into tables in other MIBs. The values of ifIndex are the same for all models, although not all indexes are supported for each model.

  The ifIndex included with the trap consists of:

  – 1 COM Port
  – 2 HDSL E1 Interface, Port 1
  – 6 G.703 Interface, Port 1

- ifAdminStatus (RFC 1573)

  This object specifies the operational state of the interface:

  – up(1)
  HDSL Network: DSL link is established.
  G.703: No alarm condition exists.

  – down(2)
  HDSL Network: DSL link is not established.
  G.703: An alarm condition exists.

  – testing(3)
  A test is active on the interface.

- ifOperStatus (RFC 1573)

  This object contains the same value as ifAdminStatus.

- ifType (RFC 1573)

  This object is the type of interface:

  – DSL(18)
  Used for the G.703 E1 interface.

Enterprise-Specific Traps

EnterpriseSpecific traps indicates that an enterprise-specific event has occurred. The Specific-trap field identifies the particular trap that occurred. The following table lists the enterprise-specific traps supported by the unit:

SNMP Trap	Description	Possible Cause
enterprisePrimary ClockFail(1)	A failure of the currently configured primary clock source for the unit has been detected.	The configured clock source is no longer operational. If the configured clock source is the internal clock, the possible cause may be due to a failure of one or more of the units hardware components.
enterpriseSecondary ClockFail(4)	A failure of the secondary clock source for the unit has been detected.	The configured clock source is no longer operational. If the configured clock source is the internal clock, the possible cause may be due to a failure of one or more of the units hardware components.
enterprisePrimary ClockFailClear(101)	Clock failure has cleared.	N/A
enterpriseSecondary ClockFailClear(104)	Clock failure has cleared.	N/A
enterpriseSelfTestFail(2)	A hardware failure of the unit is detected during the unit's self-test. The trap is generated after the unit completes initialization.	Failure of one or more of the unit's hardware components.
enterpriseDeviceFail(3)	An internal device failure.	Operating software has detected an internal device failure.
enterpriseTestStart(5)	A test is running.	At least one test has been started on an interface.
enterpriseConfig Change(6)	The configuration changed via the user interface. The trap is sent after 60 seconds have elapsed without another change. This suppresses the sending of numerous traps when multiple changes are made in a short period of time, as is typically the case when changing configuration options.	Configuration has been changed via the ATI.
enterpriseFallback AutoRate(13)	The LTU was unable to resynch to the last known rate after a loss of signal.	The transmission quality of the DSL line has degraded since the LTU last synched up.

SNMP Trap	Description	Possible Cause
enterpriseTestStop(105)	All tests have been halted.	All tests have been halted on an interface.
enterpriseFallback AutoRateClear(113)	The LTU was able to resynch to the last known rate after the enterpriseFallback AutoRate(13) was reported.	

There are no variable-bindings for enterpriseDeviceFail, enterprisePrimary ClockFail. enterpriseSecondaryClockFail, enterprisePrimaryClockFailClear, enterpriseSecondaryClockFailClear, and enterpriseConfigChange. The variable-binding for enterpriseSelfTestFail is devSelfTestResults.

The following list describes the conditions that define enterpriseFallbackAutoRate and enterpriseFallbackAutoRateClear:

enterpriseFallbackAutoRate Variable-Bindings

- ifIndex (RFC 1573)

  This object provides the index into the ifTable and potentially into tables in other MIBs. The values of ifIndex are the same for all models, although not all indexes are supported for each model.

  The ifIndex included with the trap consists of:

  – 1 COM Port
  – 2 HDSL E1 Interface, Port 1
  – 6 G.703 Interface, Port 1

- ifAdminStatus (RFC 1573)

  This object specifies the operational state of the interface:

  – up(1)
  HDSL Network: DSL link is established.
  G.703: No alarm condition exists.

  – down(2)
  HDSL Network: DSL link is not established.
  G.703: An alarm condition exists.

  – testing(3)
  A test is active on the interface.

- ifOperStatus (RFC 1573)

  This object contains the same value as ifAdminStatus.

- ifType (RFC 1573)

  This object is the type of interface:

  – e1(19)
  Used for the G.703 E1 interface.

The tests that affect the enterpriseTestStart, enterpriseTestStop, and the variable-bindings are different for each particular interface. Diagnostic tests are only supported on the physical E1 network and user data port interfaces. The specific tests and variable-bindings are described in the following table:

Interface	enterpriseTestStart/Stop Variable-Bindings	Possible Cause
HDSL Network	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifType (RFC 1573) ■ ifTestType (RFC 1573) The following objects control tests in SNMP-managed devices: – noTest – Stops the test in progress. – testLoopLLB – Initiates a Local Loopback. – testLoopRLB – Initiates a Remote Loopback. – testSendMon511 – Initiates a Send and Monitor 511 test. – testSendLLBUp – Initiates an LLB Up message to the remote unit. – testSendLLBDown – Initiates an LLB Down message to the remote unit.	■ enterpriseTest Start – Any one of the following tests is active on the interface: – Line Loopback – Payload Loopback – Repeater Loopback – Remote Line Loopback – Send and Monitor 511 ■ enterpriseTest Stop – No tests currently running on the interface.
G.703	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ ifTestType (RFC 1573) The following objects control tests in SNMP-managed devices: – noTest – Stops the test in progress. – testLoopExternalDTE	

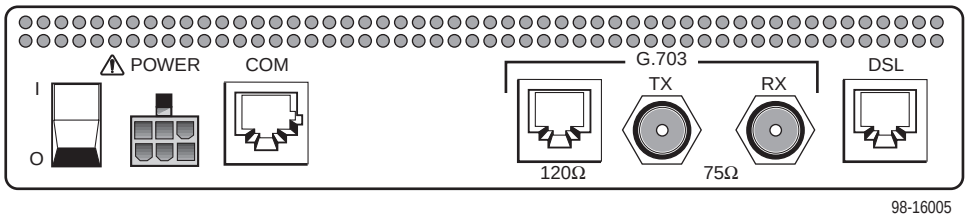
Cables and Pin Assignments

C

Overview

The following sections provide pin assignments:

- *E1 Network Interface Cable*
- *DSL Network Interface Cable and Connector*
- *COM Port Interface Cable*
- *Power Input Connector*
- *Optional Power Cable*



Hotwire 7986 Standalone Termination Unit Rear Panel

E1 Network Interface

The E1 network interface is either two BNC connectors (Transmit and Receive) for a 75-ohm unbalanced interface, or an RJ48C, 8-position, unkeyed modular connector (Table C-1, Figure C-1) for a 120-ohm balanced interface.

Table C-1. E1 120-Ohm Balanced Interface Connector

Signal	Pin Number
Receive Ring	1
Receive Tip	2
Receive Shield	7
Transmit Ring	4
Transmit Tip	5
Transmit Shield	8

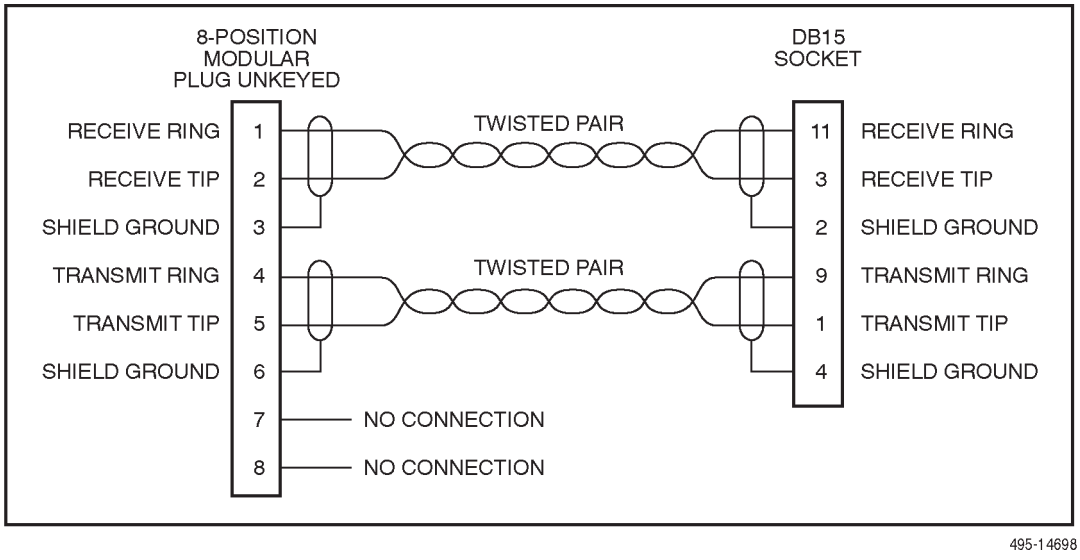


Figure C-1. E1 120-Ohm Network Interface Adapter Cable (Feature Number 3100-F1-517)

DSL Network Interface Cable

The DSL line interface cable is a 20-foot, 24 AWG solid, 2-twisted-pair cable that is RJ48C-to-RJ48C (Table C-2, Figure C-2).

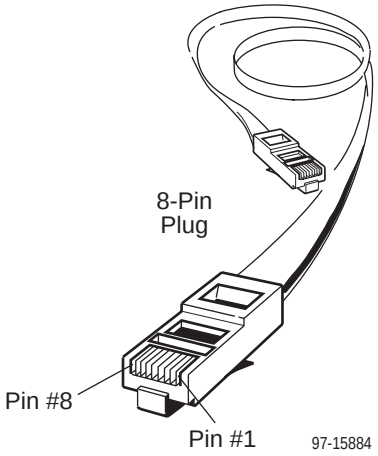


Table C-2. DSL Network Interface Connector

Signal	Pin Number
Data in (Ring)	1
Data in (Tip)	2
Data out (Ring)	4
Data out (Tip)	5

NOTE:

A crossover cable (Pins 1, 2 to 4, 5) is required for connecting two 7986 Termination Units back-to-back.

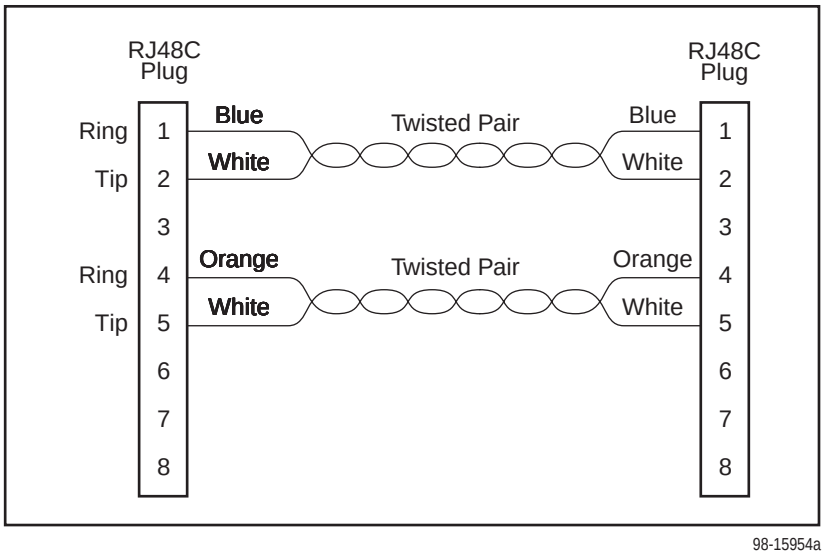


Figure C-2. DSL Network Interface Cable with RJ48C Connector (Feature Number 7900-F1-514)

COM Port Interface Cable

The COM port connects to either a PC or to an ASCII terminal or printer for alarms. The COM port-to-PC cable is a 14-foot, 26 AWG, 8-conductor cable with an 8-position modular plug keyed connector and a DB9 socket connector (Figure C-3). The COM port connector is an 8-position keyed modular jack (Table C-3). The data signals on this port are referenced to a DTE interface.

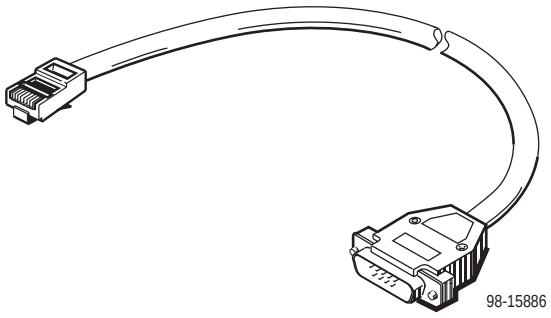


Table C-3. COM Port Interface Connector

Signal	Pin Number
Rx Data (out to DTE)	2
Ground	3
Tx Data (in from DTE)	4
DTR (in from DTE)	5
CD (out to DTE)	6
RTS (in from DTE)	7

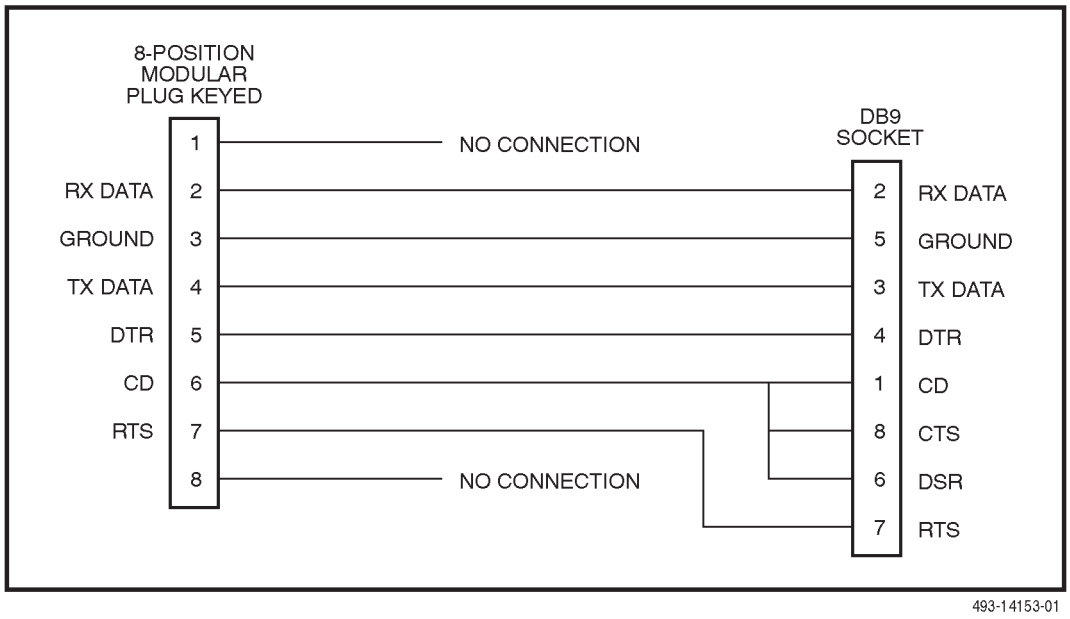


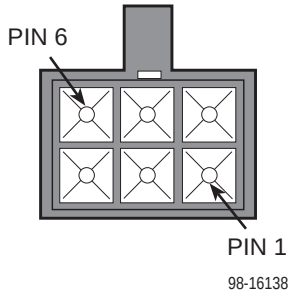
Figure C-3. COM Port-to-PC Cable (Feature Number 7900-F1-510)

Power Input Connector

The required input power connector leads are shown in Table C-4.

Table C-4. DC Power Connector

Signal	Pin Number
+24 Vdc	5
+24 Vdc Return	4
Chassis Ground	3



Optional Power Cable

The optional power cable is a 14.5-foot, 18 AWG stranded cable. The connector is terminated at one end with a 6-position Molex 39-01-2060 connector. The other end of the cable is terminated with a bare wire that should be connected to a DC power source. Figure C-4 shows the wire colors.

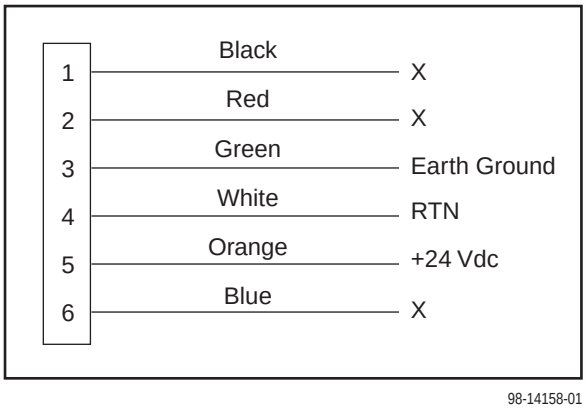


Figure C-4. DC Power Cable (Feature Number 7900-F1-506)

Technical Specifications

D

Specifications	Criteria*
Size	Width 7.25 inches (18.4 cm) Height 1.5 inches (3.8 cm) Length 9.4 inch (24.9 cm)
Weight	Approximately 1.25 lbs. (0.6 kg)
Approvals Safety Certifications	Refer to the equipment's label for approvals on product.
Power	The Model 7986 Termination Unit contains a DC-to-DC converter that requires +24V power input. The +24V power is distributed through a universal power supply supplied with the unit. Maximum Power Dissipation = 6 watts
Cables and Cable Guide	Feature Number — Description 7900-F1-506 — Optional Power Cable 7900-F1-507 — COM Port Interface Cable 7900-F1-514 — DSL Network Interface Cable
Physical Environment Operating temperature Storage temperature Relative humidity	 32° to 122° F (0° to 50° C) –4° F (–20° C) to 158° F (70° C) 5% to 85% (noncondensing)
* Technical specifications are subject to change without notice.	

Glossary

511	A random bit test 511 bytes in length.
AMI	Alternate Mark Inversion. A line coding technique used to accommodate the ones density requirements of E1 or T1 lines.
ATI	Asynchronous Terminal Interface. A menu-driven, VT100-compatible system for configuring and managing the termination unit.
BPV	Bipolar Violation. In a bipolar signal, a one (mark, pulse) which has the same polarity as its predecessor.
bridged tap	Any part of the local loop that is not in the direct talking path between the CO and the service user.
CD	Carrier Detect. The received line signal detector. V.24 circuit 109.
CO	Central Office/Central Site. The PSTN facility that houses one or more switches serving local telephone subscribers.
COM port	Communications port. A computer's serial communications port used to transmit to and receive data from a modem. The modem connects directly to this port.
CP	Customer Premises.
CPE	Customer Premises Equipment. Terminal equipment on the service user's side of the telecommunications network interface.
CPU	Central Processing Unit. The main or only computing device in a data processing system.
CRC	Cyclic Redundancy Check. A mathematical method of confirming the integrity of received digital data.
CTS	Clear To Send. A signal indicating that the device is ready for the DTE to transmit data. Usually occurs in response to Request To Send (RTS).
CV	Code Violation. Detected when using HDB3 coding format, this is equivalent to a BPV when using AMI coding.
DCE	Data Communications Equipment. The equipment that provides the functions required to establish, maintain, and end a connection. It also provides the signal conversion required for communication between the DTE and the network.
DCLB	Data Channel LoopBack. Loops the data received from the network interface, for all DS0 channels allocated to the selected port, back to the network.
DSL	Digital Subscriber Line. The non-loaded, local-loop copper connection between the customer and the first node within the network.
DSLAM	Digital Subscriber Line Access Multiplexer. A platform for DSL modems that provides high-speed data transmission over traditional twisted-pair wiring.
DSR	Data Set Ready. A signal from the modem to the DTE that indicates the modem is turned ON and connected to the DTE.
DTE	Data Terminal Equipment. The equipment, such as a computer or terminal, that provides data in the form of digital signals for transmission.

DTLB	Data Terminal Loopback. LoopBack mode that loops the data for a particular synchronous data port back to the port just before it is combined with the rest of the T1 data stream.
DTR	Data Terminal Ready. A signal from the DTE to the modem, sent via Pin 20 of the EIA-232 interface (V.24 circuit 108/1, /2), that indicates the DTE is turned ON and connected to the modem.
E1	A wideband digital interface operating at 2.048 Mbps, defined by ITU recommendations G.703 and G.704. It is used primarily outside North America.
EER	Excessive Error Rate. An error rate that is greater than the threshold that has been configured in the device.
EOC	Embedded Operations Channel. An in-band channel between DSL devices, used for 4 kbps management data.
ES	Errored Seconds. A second with one or more ESF error events (one or more CRC6 error events or OOFs).
ESF	Extended SuperFrame. The T1 transmission standard that specifies 24 frames as an extended superframe to be used for frame synchronization and to locate signaling bits.
Ethernet	A type of network that supports high-speed communication among systems. It is a widely implemented standard for LANs. All hosts are connected to a coaxial cable where they contend for network access using a Carrier Sense, Multiple Access with Collision Detection (CSMA/CD) paradigm.
ETSI	European Telecommunications Standardization Institute. An organization that produces technical standards in the area of telecommunications.
factory defaults	A predetermined set of configuration options containing the optimum settings for operation on asynchronous dial networks.
FAS	Frame Alignment Signal. A loss of signal (LOS) error detection.
FAW	Frame Alignment Word. A loss of synchronization error detection.
FCC	Federal Communications Commission. The Board of Commissioners that regulates all electrical communications that originate in the United States.
FEBE	Far-End Block Error. Block errors reported by remote equipment.
frame relay	A high-speed connection-oriented packet switching WAN protocol using variable-length frames.
FTP	File Transfer Protocol. A TCP/IP standard protocol that allows a user on one host to access and transfer files to and from another host over a network, provided that the client supplies a login identifier and password to the server.
G.703	An ITU recommendation for the physical and logical characteristics of hierarchical digital devices.
G.704	An ITU recommendation for synchronous frame structures.
HDB3	High Density Bipolar Three Zeros Substitution. A line coding technique used to accommodate the ones density requirements of E1 lines.
HDSL	High-bit-rate Digital Subscriber Line. A technique for high bandwidth, bidirectional transmission over copper wire for T1 and E1 services.
IP	Internet Protocol. An open networking protocol used for internet packet delivery.
IP address	Internet Protocol address. The address assigned to an internet host.
LAN	Local Area Network. A privately owned and administered data communications network limited to a small geographic area.

LED	Light Emitting Diode. A light or status indicator that glows in response to the presence of a certain condition (e.g., an alarm).
LLB	Line LoopBack. A test in which the received signal on the network interface is looped back to the network without change.
loopback	A diagnostic procedure that sends a test message back to its origination point. Used to test various portions of a data link in order to isolate an equipment or data line problem.
LOS	Loss of Signal. The T1 line condition where there are no pulses.
LTU	Line Termination Unit. The control unit on the network end of a link. (The NTU is on the customer premises end.)
MCC	Management Communications Controller. The DSLAM circuit card used to configure and monitor the DSLAM.
MIB	Management Information Base. A database of managed objects used by SNMP to provide network management information and device control.
MIB II	MIB Release 2. The current Internet-standard MIB, defined by RFC 1213.
M/SDSL	Multirate SDSL.
MTSO	Mobile Telephone Switching Office. A generic name for the main cellular switching center which supports multiple base stations.
NMS	Network Management System. A computer system used for monitoring and controlling network devices.
NTU	Network Termination Unit. The unit on the customer premises end of a link. (The LTU is on the network end.)
OOF	Out Of Frame. An error condition in which frame synchronization bits are in error.
reset	A reinitialization of the device that occurs at power-up or in response to a reset command.
RLB	Repeater LoopBack. Loops the signal being sent to the network back to the DTE Drop/Insert and data ports after it has passed through the framing circuitry of the device.
router	A device that connects LANs by dynamically routing data according to destination and available routes.
RTS	Request to Send. A signal from the DTE to the device, indicating that the DTE has data to send. V.24 circuit 105.
RXD	Received Data. Pin 3 of the EIA-232 interface that is used by the DTE to receive data from the modem. Conversely, the modem uses Pin 3 to transmit data to the DTE.
SDSL	Symmetrical Digital Subscriber Line. A technique for the use of an existing twisted pair line that permits high bandwidth, bidirectional transmission.
SES	Severely Errored Seconds. Usually defined as a second during which a specific number of CRC errors was exceeded, or an OOF or other critical error occurred.
SNMP	Simple Network Management Protocol. Protocol for open networking management.
TCP/IP	Transmission Control Protocol/Internet Protocol. The dominant protocol suite in the worldwide Internet, TCP allows a process on one machine to send data to a process on another machine using the IP. TCP can be used as a full-duplex or one-way simplex connection.
Telnet	Virtual terminal protocol in the Internet suite of protocols. Allows the user of one host computer to log into a remote host computer and interact as a normal terminal user for that host.

TFTP Trivial File Transfer Protocol. A standard TCP/IP protocol that allows simple file transfer to and from a remote system without directory or file listing. TFTP is used where FTP is not available.

TXD Transmit Data. Pin 2 of the EIA-232 interface that is used by the DTE to transmit data to the modem. Conversely, the modem uses Pin 2 to receive data from the DTE.

UNIX An operating system developed at AT&T Bell Laboratories and since used as the basis of similar operating systems.

WAN Wide Area Network. A network that spans a large geographic area.

Index

A

Abort All Tests, 5-1
ac transformer, connecting, 3-2
access
  SNMP, 7-4
  to async terminal interface, 2-3
access level
  effective, 7-1
  functions available for, 7-1
access to user interface, resetting/restoring, 7-5
administer login, 7-2
AIS (Alarm Indication Signal), status message, 4-3
Alarm, LED, 4-14
ASCII, printable characters, 3-4
ATI (Asynchronous Terminal Interface)
  access, 2-1
  defined, 1-2
  exiting, 2-9
  initiating session, 2-2
  virtual function keys, 2-7
authentificationFailure, B-1
AutoRate, 3-13, A-2

C

Cables
  COM Port Interface Cable, C-4
  DSL Network Interface Cable, C-3
  Optional Power Cable, C-5
cables, C-1
  figures, C-1
  part numbers, D-1
  pin Assignments, C-1
cabling
  COM Port-to-PC cable, C-4
  DC Power cable, C-5
  DSL Network Interface Cable, C-3
Card Failed
  self-test result, 4-5
  status message, 4-4
Circuit Identifier, A-3
Clock Failed, status message, 4-4
COM port, resetting, 7-5
COM port settings, 3-3
Communication Port, A-8
Community Name , A-19, A-20
Community Name 1, A-19
Community Name 2, A-20
community names, for SNMP, 7-4
Configurating AutoRate, 3-13
Configuring the unit, 3-1
configuration
  example, 1-3
  General SNMP Management Options, A-19
  option tables, A-1
  SNMP Management, A-19
  SNMP NMS Security Options, A-19, A-21
configuration changes, saving, 3-17
Configuration Edit/Display, 3-12
Configuration Loader, 3-15
Configuration menu, 3-11
Configuration Mode, choosing an interface mode, 3-6
Configuration Options, accessing, 3-11
configuration options
  Communication Port, A-8
  G.703 Interface, A-4
  System Options, A-6
Connecting to the Network, 3-3
connectors
  Location, 1-4
  power input, C-5
  rear panel, C-1
CPU Fail, self-test result, 4-5
create login ID, 7-2
customer configuration, 3-6
  switchpacks, internal switches, 3-7

D

dc power option, 3-2– 3-18
default configuration area, 3-6
delete, Login ID, 7-4
device, messages, 6-3– 6-4
dimensions, D-1
Disconnect Time, for Telnet session, A-10, A-12
documents, related, vi
DOS, TFTP server on, 3-15
download code, 3-18
Download Failed, status message, 4-4
DSL Line Rate, 3-10
    Fixed Rate, 3-14
DSL Line Rates, 3-14
DSL Port, LEDs, 4-14
DSLAM, defined, 1-2
DTE loopback , 5-5

E

EER (Excessive Error Rate) , status message, 4-3
effective access level, 7-1
ending an ATI session, 2-9
enterprise, SNMP traps, B-3
environment requirements, D-1
error messages, line 24, 6-3
error statistics, 4-7
ESD precautions, 3-7
Excessive Error Rate (EER) Threshold, A-2, A-5

F

factory default configuration options, resetting, 7-5
factory defaults, 3-6
Failure, self-test result, 4-5
feature numbers, D-1
features, 1-2
firmware, download from server, 3-18
Front Panel LEDs, 1-4

G

G.703 Interface Impedance, A-7
G.703 Interface Options, A-4
G.703 Interface Option settings, A-4
    Port Status, A-4
G.703 Props, LEDs, 4-14
General SNMP Traps Options, A-19

H

health and status messages, 4-3

I

identity, 3-4
Impedance, A-7
inactivity timeout, for Telnet session, A-10, A-12
Initial Startup and Configuration, 3-1
intended audience, v
Internal Switches, 3-7
Manual configuration, Internal Switches, 3-7
IP address
    DSL peer, A-3
    SNMP manager, 7-5
IP addresses, 8-1
IP addressing, example, 8-2

K

keyboard functions, 2-6

L

lamp test, 5-8
LEDs, 4-13, 4-14
Line Coding Format, A-4
Line Framing , A-5
Link Up, LEDs, 4-14
link-layer protocols, 8-1
linkUp and linkDown traps, B-2
local line loopback (LLB), 5-3
LOF (Loss Of Frame), status message, 4-3
Login ID
    access levels, 7-1
    adding, 7-2
    deleting, 7-4
login ID, 7-1
loopback, effect on LEDs, 4-14
LOS (Loss Of Signal), status message, 4-3

M

main menu, 2-2, A-1
Management and Communication Options, A-11
management port
  access, 7-1
  settings, 2-1
Margin Threshold, A-2
Memory Fail, status, 4-5
messages
  alarm and device, 6-1
  health and status, 4-3
  line 24, 6-3
  self-test results, 4-5
  test status, 4-6
MIB
  general support, 1-5
  support, 1-5
monitoring, 4-1

N

navigating the screens, 2-6
Net Margin Threshold, status message, 4-3
network
  interface options, A-2
  tests, 5-2
G.703 Failed, self-test result, 4-5
network interface, pin assignments, C-2– C-6
network interface options, A-3
Network-Initiated DCLB, A-5
NMS
  SNMP access, 7-5
  SNMP connectivity, 8-1
no test active status message, 4-6

O

OK, LED, 4-14
OOF (Out Of Frame), status message, 4-3
options, configuration tables, A-1
overview
  8775 Termination Unit, 1-2
  user's guide, v

P

part numbers, D-1
Passed, self-test result, 4-5
Payload Rates, 3-14
PC
  connecting, 3-3
  requirements, 3-3
Peer IP Address, A-3
performance statistics, 4-9
  G.703, 4-11
physical environment requirements, D-1
pin assignments, C-1
port, COM, C-4
Port Status , A-4
power cord installation, 3-2
power input, optional power sources, 3-2– 3-18
power requirements, D-1
power supply
  ac transformer, 3-2
  optional dc, 3-2– 3-18

R

Rear Panel, 1-4
related documents, vi
remote send line loopback, 5-6
repeater loopback (RLB), 5-4
resetting
  the access unit, COM port, 7-5
  the unit, default configuration options, 7-5
restoring, user interface access, 7-5

S

Save Configuration screen, 3-17
saving option changes, 3-17
screen, function keys, 2-7
screens, for user interface, 2-1– 2-6
SDSL Mode, A-6
security, 7-1
self-test results, 4-5
Send and Monitor 511, 5-7
Send Remote Line Loopback, 5-6
size of unit, D-1
SNMP
  trap options, 6-2
  traps, B-1

SNMP Management Configuration, A-19
SNMP management
  general, 1-5
  limiting access, 7-4
SNMP NMS Security Options, A-19, A-21
SNMP Trap Options, NMS n IP Address, A-22
start-up, ATI, 2-1
status, test messages, 4-6
subnet, IP addresses, 8-1
Switchpack definitions, 3-9
Switchpack locations, 3-8
Switchpack S1 Definitions, 3-9
Switchpack S2 Definitions, 3-10
system, LEDs, 4-14
System Options, A-6

T

Telnet session
  access level, A-12, A-14
  enable/disable, A-12, A-14
  inactivity timeout, A-10, A-12
  login required, A-12, A-14
telnet session access, 7-1
telnet session options, A-11, A-13
terminal
  communication parameters, 3-3
  connecting, 3-3
terminal port, direct connection, 2-1
test
  aborting, 5-9
  DTE Loopback, 5-5
  LED, 4-14
  Line Loopback, 5-3
  Network-Initiated DCLB, A-5
  Remote Send Line Loopback, 5-6
  Repeater Loopback, 5-4
  Send and Monitor 511, 5-7
  status messages, 4-6
  terminating, 5-9
  Test Duration, A-7
  Test Timeout, A-6
Test menu, 5-2
testing, 5-1
timeout
  Com port session inactivity, A-10
  Telnet session inactivity, A-12
traps, SNMP, 6-2, B-1
troubleshooting, 6-5
  DSL performance statistics, 4-9
  error statistics, 4-7
  G.703 performance statistics, 4-11

U

UNIX, TFTP server on, 3-15
user interface, 3-3
  async terminal, 2-1
  how to access, 2-1
  resetting/restoring access, 7-5

V

virtual function keys, 2-7

W

warmStart, B-1
weight of unit, D-1